

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-187101

(43)Date of publication of application : 04.07.2003

(51)Int.Cl.

G06F 17/60
H04L 9/32
H04N 7/167
H04N 7/173

(21)Application number : 2001-385453 (71)Applicant : SONY CORP

(22)Date of filing : 19.12.2001 (72)Inventor : CHIN KOGUN

(54) INFORMATION PROCESSOR, INFORMATION PROCESSING METHOD, STORAGE MEDIUM, INFORMATION PROCESSING SYSTEM AND PROGRAM

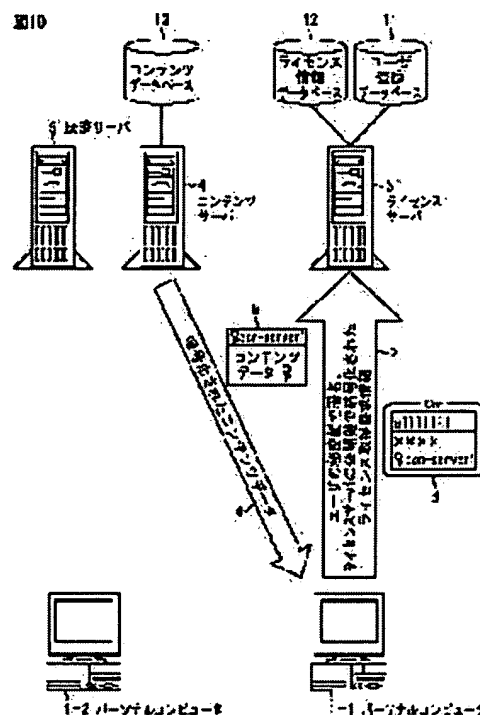
(57)Abstract:

PROBLEM TO BE SOLVED: To protect a copyright of a content when making content transferable by peer-to-peer.

SOLUTION: Transmission and receipt of encrypted content data between a content server 4 and a personal computer 1-1 is executed without using public key cryptosystem as shown by (a) in a Figure. User information containing information ID showing the source of the content data is described in a field attached to the content data as shown by b in the Figure. Since the user information is encrypted by the public key of a license server 3, only the license server 3 can read it.

Electronically signed preview license acquisition request information or general license acquisition request

information is transmitted to the license server 3 as shown by c in the Figure. The information showing the source of the content data is described in the license acquisition request information as shown by d in the Figure.



LEGAL STATUS

[Date of request for examination]

THIS PAGE BLANK (USPTO)

↓ [Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

THIS PAGE BLANK (USPTO)

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-187101

(P 2 0 0 3 - 1 8 7 1 0 1 A)

(43) 公開日 平成15年7月4日 (2003. 7. 4)

(51) Int. Cl. ⁷	識別記号	F I	テ-マコード	(参考)
G06F 17/60	312	G06F 17/60	312	5C064
	142		142	5J104
	302		302	E
	512		512	
	ZEC		ZEC	

審査請求 未請求 請求項の数26 O L (全29頁) 最終頁に続く

(21) 出願番号 特願2001-385453 (P 2001-385453)

(22) 出願日 平成13年12月19日 (2001. 12. 19)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 陳 向群

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(74) 代理人 100082131

弁理士 稲本 義雄

Fターム (参考) 5C064 BA07 BB02 BB07 BC01 BC17

BC18 BC22 BC23 BD02 BD08

BD09 CA14 CB01 CC01 CC04

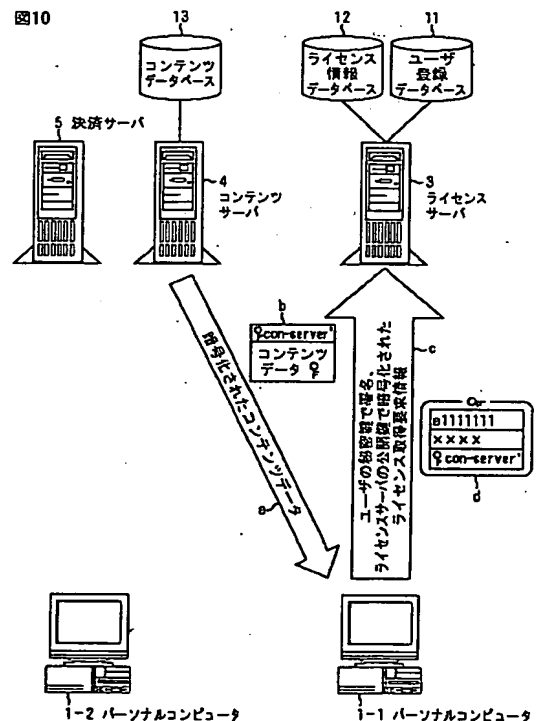
5J104 AA09 LA03 LA06 MA05

(54) 【発明の名称】 情報処理装置および情報処理方法、記録媒体、情報処理システム、並びに、プログラム

(57) 【要約】

【課題】 コンテンツをピアツーピアで授受可能とした場合にその著作権を守る。

【解決手段】 図中aに示されるように、コンテンツサーバ4とパーソナルコンピュータ1-1との暗号化されたコンテンツデータの送受信は、公開鍵暗号方式を用いずに実行される。図中bに示されるように、コンテンツデータに添付しているフィールドには、このコンテンツデータの配信元を示す情報 (ID) を含むユーザ情報が記載されている。ユーザ情報は、ライセンスサーバ3の公開鍵で暗号化されているため、ライセンスサーバ3しか読み取ることが出来ない。暗号化され、電子署名されたプレビューライセンス取得要求情報、もしくは通常ライセンス取得要求情報は、図中cに示されるように、ライセンスサーバ3に送信される。ライセンス取得要求情報には、図中dに示されるように、コンテンツデータの配信元を示す情報が記載されている。



【特許請求の範囲】

【請求項 1】 コンテンツを取得する取得手段と、
前記コンテンツに添付されている第 1 の情報、前記コンテンツを特定するための第 2 の情報、および自分自身を特定することができる第 3 の情報を含む第 4 の情報を生成する生成手段と、

前記生成手段により生成された前記第 4 の情報を送信する第 1 の送信手段と、

前記コンテンツを再生するために必要な第 5 の情報を受信する受信手段と、

前記受信手段により受信された前記第 5 の情報に添付されている第 6 の情報を抽出する抽出手段と、

前記抽出手段により抽出された前記第 6 の情報を、前記コンテンツに添付されている前記第 1 の情報に代わって、前記コンテンツに添付させる情報添付手段とを備えることを特徴とする情報処理装置。

【請求項 2】 前記情報添付手段により前記第 6 の情報が添付された前記コンテンツを、他の情報処理装置に送信する第 2 の送信手段を更に備えることを特徴とする請求項 1 に記載の情報処理装置。

【請求項 3】 前記第 1 の情報、および前記第 6 の情報は、前記第 4 の情報の送信先の公開鍵で暗号化されていることを特徴とする請求項 1 に記載の情報処理装置。

【請求項 4】 前記第 5 の情報は、前記コンテンツを条件付で再生させるための第 1 のライセンス情報と、前記コンテンツを完全に再生させるための第 2 のライセンス情報のいずれかであることを特徴とする請求項 1 に記載の情報処理装置。

【請求項 5】 前記生成手段により生成された前記第 4 の情報を、暗号化する暗号化手段を更に備えることを特徴とする請求項 1 に記載の情報処理装置。

【請求項 6】 前記暗号化手段は、前記第 4 の情報を、前記第 4 の情報の送信先の公開鍵で暗号化し、自分自身の秘密鍵で電子署名を施すことを特徴とする請求項 5 に記載の情報処理装置。

【請求項 7】 前記受信手段により受信された前記第 5 の情報を復号する復号手段を更に備えることを特徴とする請求項 1 に記載の情報処理装置。

【請求項 8】 コンテンツの取得を制御する取得制御ステップと、

前記コンテンツに添付されている第 1 の情報、前記コンテンツを特定するための第 2 の情報、および自分自身を特定することができる第 3 の情報を含む第 4 の情報を生成する生成ステップと、

前記生成ステップの処理により生成された前記第 4 の情報の送信を制御する送信制御ステップと、

前記コンテンツを再生するために必要な第 5 の情報の受信を制御する受信制御ステップと、

前記受信制御ステップの処理により受信が制御された前記第 5 の情報に添付されている第 6 の情報を抽出する抽

出ステップと、

前記抽出ステップの処理により抽出された前記第 6 の情報を、前記コンテンツに添付されている前記第 1 の情報に代わって、前記コンテンツに添付させる情報添付ステップとを含むことを特徴とする情報処理方法。

【請求項 9】 コンテンツの取得を制御する取得制御ステップと、

前記コンテンツに添付されている第 1 の情報、前記コンテンツを特定するための第 2 の情報、および自分自身を特定することができる第 3 の情報を含む第 4 の情報を生成する生成ステップと、

前記生成ステップの処理により生成された前記第 4 の情報の送信を制御する送信制御ステップと、

前記コンテンツを再生するために必要な第 5 の情報の受信を制御する受信制御ステップと、

前記受信制御ステップの処理により受信が制御された前記第 5 の情報に添付されている第 6 の情報を抽出する抽出ステップと、

前記抽出ステップの処理により抽出された前記第 6 の情報を、前記コンテンツに添付されている前記第 1 の情報に代わって、前記コンテンツに添付させる情報添付ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項 10】 コンテンツの取得を制御する取得制御ステップと、

前記コンテンツに添付されている第 1 の情報、前記コンテンツを特定するための第 2 の情報、および自分自身を特定することができる第 3 の情報を含む第 4 の情報を生成する生成ステップと、

前記生成ステップの処理により生成された前記第 4 の情報の送信を制御する送信制御ステップと、

前記コンテンツを再生するために必要な第 5 の情報の受信を制御する受信制御ステップと、

前記受信制御ステップの処理により受信が制御された前記第 5 の情報に添付されている第 6 の情報を抽出する抽出ステップと、

前記抽出ステップの処理により抽出された前記第 6 の情報を、前記コンテンツに添付されている前記第 1 の情報に代わって、前記コンテンツに添付させる情報添付ステップとを含む処理をコンピュータに実行させることを特徴とするプログラム。

【請求項 11】 コンテンツを取得する取得手段と、
前記コンテンツに添付されている第 1 の情報、前記コンテンツを特定するための第 2 の情報、および自分自身を特定することができる第 3 の情報を含む第 4 の情報を生成する生成手段と、

前記生成手段により生成された前記第 4 の情報を送信する送信手段と、

前記コンテンツを再生するために必要な第 5 の情報を受信する受信手段と、

10

20

30

40

50

自分自身を特定することができる第 6 の情報を、前記第 4 の情報の送信先の公開鍵で暗号化する暗号化手段と、前記暗号化手段により暗号化された前記第 6 の情報を、前記コンテンツに添付されている前記第 1 の情報に代わって、前記コンテンツに添付させる情報添付手段とを備えることを特徴とする情報処理装置。

【請求項 12】 コンテンツの取得を制御する取得制御ステップと、

前記コンテンツに添付されている第 1 の情報、前記コンテンツを特定するための第 2 の情報、および自分自身を特定することができる第 3 の情報を含む第 4 の情報を生成する生成ステップと、

前記生成ステップの処理により生成された前記第 4 の情報の送信を制御する送信制御ステップと、

前記コンテンツを再生するために必要な第 5 の情報の受信を制御する受信制御ステップと、

自分自身を特定することができる第 6 の情報を、前記第 4 の情報の送信先の公開鍵で暗号化する暗号化ステップと、

前記暗号化ステップの処理により暗号化された前記第 6 の情報を、前記コンテンツに添付されている前記第 1 の情報に代わって、前記コンテンツに添付させる情報添付ステップとを含むことを特徴とする情報処理方法。

【請求項 13】 コンテンツの取得を制御する取得制御ステップと、

前記コンテンツに添付されている第 1 の情報、前記コンテンツを特定するための第 2 の情報、および自分自身を特定することができる第 3 の情報を含む第 4 の情報を生成する生成ステップと、

前記生成ステップの処理により生成された前記第 4 の情報の送信を制御する送信制御ステップと、

前記コンテンツを再生するために必要な第 5 の情報の受信を制御する受信制御ステップと、

自分自身を特定することができる第 6 の情報を、前記第 4 の情報の送信先の公開鍵で暗号化する暗号化ステップと、

前記暗号化ステップの処理により暗号化された前記第 6 の情報を、前記コンテンツに添付されている前記第 1 の情報に代わって、前記コンテンツに添付させる情報添付ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項 14】 コンテンツの取得を制御する取得制御ステップと、

前記コンテンツに添付されている第 1 の情報、前記コンテンツを特定するための第 2 の情報、および自分自身を特定することができる第 3 の情報を含む第 4 の情報を生成する生成ステップと、

前記生成ステップの処理により生成された前記第 4 の情報の送信を制御する送信制御ステップと、

前記コンテンツを再生するために必要な第 5 の情報の受

信を制御する受信制御ステップと、

自分自身を特定することができる第 6 の情報を、前記第 4 の情報の送信先の公開鍵で暗号化する暗号化ステップと、

前記暗号化ステップの処理により暗号化された前記第 6 の情報を、前記コンテンツに添付されている前記第 1 の情報に代わって、前記コンテンツに添付させる情報添付ステップとを含む処理をコンピュータに実行させることを特徴とするプログラム。

10 【請求項 15】 コンテンツを再生させるために用いられる、前記コンテンツに固有の第 1 の情報を記録する第 1 の記録手段と、

前記コンテンツを保有する他の情報処理装置から、前記コンテンツに添付されている第 2 の情報、前記コンテンツを特定するための第 3 の情報、および、前記他の情報処理装置を特定するための第 4 の情報を含む第 5 の情報を受信する受信手段と、

前記第 1 の記録手段に記録されている前記第 1 の情報のうち、前記第 3 の情報によって特定される前記コンテンツに対応する前記第 1 の情報を抽出する抽出手段と、

20 前記他の情報処理装置を特定する情報を少なくとも含む第 6 の情報を生成する第 1 の生成手段と、

前記第 1 の生成手段により生成された前記第 6 の情報、および前記抽出手段により抽出された前記第 1 の情報を少なくとも含む第 7 の情報を生成する第 2 の生成手段と、

前記第 2 の生成手段により生成された前記第 7 の情報を前記第 4 の情報により特定される前記他の情報処理装置へ送信する送信手段とを備えることを特徴とする情報処理装置。

30 【請求項 16】 前記第 1 の生成手段により生成された前記第 6 の情報を、自分自身の公開鍵で暗号化する暗号化手段を更に備え、

前記第 2 の生成手段は、前記暗号化手段により暗号化された前記第 6 の情報、および前記抽出手段により抽出された前記第 1 の情報を少なくとも含む第 7 の情報を生成することを特徴とする請求項 15 に記載の情報処理装置。

40 【請求項 17】 前記受信手段により受信された前記第 5 の情報に含まれている前記第 2 の情報を自分自身の秘密鍵を用いて復号する復号手段を更に備え、

前記第 2 の情報は、前記公開鍵により暗号化されている情報であることを特徴とする請求項 15 に記載の情報処理装置。

【請求項 18】 前記第 1 の情報は、前記コンテンツを条件付で再生させるための第 1 のライセンス情報と、前記コンテンツを完全に再生させるための第 2 のライセンス情報のいずれかであることを特徴とする請求項 15 に記載の情報処理装置。

50 【請求項 19】 前記第 2 の生成手段により生成された

前記第 7 の情報を暗号化する暗号化手段を更に備えることを特徴とする請求項 15 に記載の情報処理装置。

【請求項 20】 前記暗号化手段は、前記第 7 の情報を、前記第 4 の情報により特定される前記他の情報処理装置の公開鍵で暗号化し、自分自身の秘密鍵で電子署名を施すことを特徴とする請求項 19 に記載の情報処理装置。

【請求項 21】 前記受信手段により受信された前記第 5 の情報を復号する復号手段を更に備えることを特徴とする請求項 15 に記載の情報処理装置。

【請求項 22】 前記受信手段により受信された前記第 5 の情報に含まれている、前記第 2 の情報、前記第 3 の情報、および前記第 4 の情報を記録する第 2 の記録手段と、

前記第 2 の記録手段により記録された前記第 2 の情報、前記第 3 の情報、および前記第 4 の情報を基に、前記コンテンツに関する情報を解析する解析手段とを更に備えることを特徴とする請求項 15 に記載の情報処理装置。

【請求項 23】 コンテンツを再生させるために用いられる、前記コンテンツに固有の第 1 の情報の記録を制御する記録制御ステップと、

前記コンテンツを保有する他の情報処理装置からの、前記コンテンツに添付されている第 2 の情報、前記コンテンツを特定するための第 3 の情報、および、前記他の情報処理装置を特定するための第 4 の情報を含む第 5 の情報の受信を制御する受信制御ステップと、

前記記録制御ステップの処理により記録が制御されている前記第 1 の情報のうち、前記第 3 の情報によって特定される前記コンテンツに対応する前記第 1 の情報を抽出する抽出ステップと、

前記他の情報処理装置を特定する情報を少なくとも含む第 6 の情報を生成する第 1 の生成ステップと、

前記第 1 の生成ステップの処理により生成された前記第 6 の情報、および前記抽出ステップの処理により抽出された前記第 1 の情報を少なくとも含む第 7 の情報を生成する第 2 の生成ステップと、

前記第 2 の生成ステップの処理により生成された前記第 7 の情報の、前記第 4 の情報により特定される前記他の情報処理装置への送信を制御する送信制御ステップとを含むことを特徴とする情報処理方法。

【請求項 24】 コンテンツを再生させるために用いられる、前記コンテンツに固有の第 1 の情報の記録を制御する記録制御ステップと、

前記コンテンツを保有する他の情報処理装置からの、前記コンテンツに添付されている第 2 の情報、前記コンテンツを特定するための第 3 の情報、および、前記他の情報処理装置を特定するための第 4 の情報を含む第 5 の情報の受信を制御する受信制御ステップと、

前記記録制御ステップの処理により記録が制御されている前記第 1 の情報のうち、前記第 3 の情報によって特定

される前記コンテンツに対応する前記第 1 の情報を抽出する抽出ステップと、

前記他の情報処理装置を特定する情報を少なくとも含む第 6 の情報を生成する第 1 の生成ステップと、

前記第 1 の生成ステップの処理により生成された前記第 6 の情報、および前記抽出ステップの処理により抽出された前記第 1 の情報を少なくとも含む第 7 の情報を生成する第 2 の生成ステップと、

前記第 2 の生成ステップの処理により生成された前記第 7 の情報の、前記第 4 の情報により特定される前記他の情報処理装置への送信を制御する送信制御ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項 25】 コンテンツを再生させるために用いられる、前記コンテンツに固有の第 1 の情報の記録を制御する記録制御ステップと、

前記コンテンツを保有する他の情報処理装置からの、前記コンテンツに添付されている第 2 の情報、前記コンテンツを特定するための第 3 の情報、および、前記他の情報処理装置を特定するための第 4 の情報を含む第 5 の情報の受信を制御する受信制御ステップと、

前記記録制御ステップの処理により記録が制御されている前記第 1 の情報のうち、前記第 3 の情報によって特定される前記コンテンツに対応する前記第 1 の情報を抽出する抽出ステップと、

前記他の情報処理装置を特定する情報を少なくとも含む第 6 の情報を生成する第 1 の生成ステップと、

前記第 1 の生成ステップの処理により生成された前記第 6 の情報、および前記抽出ステップの処理により抽出された前記第 1 の情報を少なくとも含む第 7 の情報を生成する第 2 の生成ステップと、

前記第 2 の生成ステップの処理により生成された前記第 7 の情報の、前記第 4 の情報により特定される前記他の情報処理装置への送信を制御する送信制御ステップとを含む処理をコンピュータに実行させることを特徴とするプログラム。

【請求項 26】 コンテンツを取得して再生する、少なくとも一つの第 1 の情報処理装置と、

前記コンテンツを再生させるための情報を前記第 1 の情報処理装置に送信する第 2 の情報処理装置とによって構成される情報処理システムにおいて、

前記第 1 の情報処理装置は、

前記コンテンツを取得する取得手段と、

前記コンテンツに添付されている第 1 の情報、前記コンテンツを特定するための第 2 の情報、および自分自身を特定することができる第 3 の情報を含む第 4 の情報を生成する第 1 の生成手段と、

前記第 1 の生成手段により生成された前記第 4 の情報を前記第 2 の情報処理装置へ送信する第 1 の送信手段と、前記第 2 の情報処理装置から送信された前記コンテンツ

を再生するために必要な第 5 の情報を受信する第 1 の受信手段と、
前記受信手段により受信された前記第 5 の情報に添付されている第 6 の情報を抽出する第 1 の抽出手段と、
前記第 1 の抽出手段により抽出された前記第 6 の情報を、前記コンテンツに添付されている前記第 1 の情報に代わって、前記コンテンツに添付させる情報添付手段とを備え、
前記第 2 の情報処理装置は、
前記コンテンツを再生させるために用いられる、前記コンテンツに固有の第 7 の情報を記録する記録手段と、
前記第 1 の情報処理装置から、前記第 1 の情報、前記第 2 の情報、および、
前記第 3 の情報を含む前記第 4 の情報を受信する第 2 の受信手段と、
前記記録手段に記録されている前記第 7 の情報のうち、前記第 2 の情報によって特定される前記コンテンツに対応する前記第 7 の情報を抽出する第 2 の抽出手段と、
前記第 1 の情報処理装置を特定する情報を少なくとも含む前記第 6 の情報を生成する第 2 の生成手段と、
前記第 2 の生成手段により生成された前記第 6 の情報、および前記第 2 の抽出手段により抽出された前記第 7 の情報を少なくとも含む前記第 5 の情報を生成する第 3 の生成手段と、
前記第 3 の生成手段により生成された前記第 5 の情報を前記第 3 の情報により特定される前記第 1 の情報処理装置へ送信する第 2 の送信手段とを備えることを特徴とする情報処理システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、情報処理装置および情報処理方法、記録媒体、情報処理システム、並びに、プログラムに関し、特に、サービスを受けるユーザ同士でコンテンツをピアツーピアで授受することが可能なコンテンツ配信サービスを提供する場合に用いて好適な情報処理装置および情報処理方法、記録媒体、情報処理システム、並びに、プログラムに関する。

【0002】

【従来の技術】パーソナルコンピュータの記憶容量の増加、および音声や映像の再生技術の向上にともなって、パーソナルコンピュータ内部に楽曲データや映像データなどを記録し、再生して楽しむユーザが増えている。

【0003】楽曲データや映像データなど、いわゆるコンテンツデータは、インターネットなどを介して、コンテンツ配信サービスを行っている事業者が運営するウェブサイトからダウンロードすることができる。また、パーソナルコンピュータ間で、コンテンツをピアツーピアで授受することも可能である。

【0004】

【発明が解決しようとする課題】しかしながら、ユーザ

が保有するパーソナルコンピュータ間で、コンテンツをピアツーピアで授受する場合、コンテンツの著作権を守るのが非常に困難である。そのため、許可されたユーザ（例えば、料金を支払ったユーザ）に、復号鍵とともに、暗号化されたコンテンツデータを配信することが考えられている。

【0005】しかしながら、コンテンツデータを暗号化して、ピアツーピアでコンテンツデータを受け取ったユーザが、コンテンツデータを視聴することが出来ないようにしてしまえば、ピアツーピアを利用してコンテンツを広く流通させることが出来なくなる。

【0006】更に、ユーザは、料金を支払う前に、そのコンテンツデータは自分の嗜好にあったものか否かを確認するために、例えば、音楽データであれば試聴するなどして、コンテンツデータの内容を確認したいと考える。そのため、コンテンツ配信サービス事業者は、暗号化されたコンテンツデータとは別に、例えば、復号鍵を用いることなく視聴することができる試聴用データ（例えば、コンテンツデータの一部など）を配信する必要があると生じている。

【0007】本発明はこのような状況に鑑みてなされたものであり、コンテンツデータの購入前にユーザにコンテンツの試聴を可能とし、コンテンツの著作権を守りつつ、ピアツーピアを利用して、コンテンツを広く流通させることができるようにし、更に、コンテンツの流れをトレーシングすることができるようにするものである。

【0008】

【課題を解決するための手段】本発明の第 1 の情報処理装置は、コンテンツを取得する取得手段と、コンテンツに添付されている第 1 の情報、コンテンツを特定するための第 2 の情報、および自分自身を特定することができる第 3 の情報を含む第 4 の情報を生成する生成手段と、生成手段により生成された第 4 の情報を送信する第 1 の送信手段と、コンテンツを再生するために必要な第 5 の情報を受信する受信手段と、受信手段により受信された第 5 の情報に添付されている第 6 の情報を抽出する抽出手段と、抽出手段により抽出された第 6 の情報を、コンテンツに添付されている第 1 の情報に代わって、コンテンツに添付させる情報添付手段とを備えることを特徴とする。

【0009】情報添付手段により第 6 の情報が添付されたコンテンツを、他の情報処理装置に送信する第 2 の送信手段を更に備えるようにすることができる。

【0010】第 1 の情報、および第 6 の情報は、第 4 の情報の送信先の公開鍵で暗号化されているものとすることができる。

【0011】第 5 の情報は、コンテンツを条件付で再生させるための第 1 のライセンス情報と、コンテンツを完全に再生させるための第 2 のライセンス情報のいずれかであるものとすることができる。

【0012】生成手段により生成された第4の情報を、暗号化する暗号化手段を更に備えるようにすることができる。

【0013】暗号化手段には、第4の情報を、第4の情報の送信先の公開鍵で暗号化させ、自分自身の秘密鍵で電子署名を施させるようにすることができる。

【0014】受信手段により受信された第5の情報を復号する復号手段を更に備えさせるようにすることができる。

【0015】本発明の第1の情報処理方法は、コンテンツの取得を制御する取得制御ステップと、コンテンツに添付されている第1の情報、コンテンツを特定するための第2の情報、および自分自身を特定することができる第3の情報を含む第4の情報を生成する生成ステップと、生成ステップの処理により生成された第4の情報の送信を制御する送信制御ステップと、コンテンツを再生するために必要な第5の情報の受信を制御する受信制御ステップと、受信制御ステップの処理により受信が制御された第5の情報に添付されている第6の情報を抽出する抽出ステップと、抽出ステップの処理により抽出された第6の情報を、コンテンツに添付されている第1の情報に代わって、コンテンツに添付させる情報添付ステップとを含むことを特徴とする。

【0016】本発明の第1の記録媒体に記録されているプログラムは、コンテンツの取得を制御する取得制御ステップと、コンテンツに添付されている第1の情報、コンテンツを特定するための第2の情報、および自分自身を特定することができる第3の情報を含む第4の情報を生成する生成ステップと、生成ステップの処理により生成された第4の情報の送信を制御する送信制御ステップと、コンテンツを再生するために必要な第5の情報の受信を制御する受信制御ステップと、受信制御ステップの処理により受信が制御された第5の情報に添付されている第6の情報を抽出する抽出ステップと、抽出ステップの処理により抽出された第6の情報を、コンテンツに添付されている第1の情報に代わって、コンテンツに添付させる情報添付ステップとを含むことを特徴とする。

【0017】本発明の第1のプログラムは、コンテンツの取得を制御する取得制御ステップと、コンテンツに添付されている第1の情報、コンテンツを特定するための第2の情報、および自分自身を特定することができる第3の情報を含む第4の情報を生成する生成ステップと、生成ステップの処理により生成された第4の情報の送信を制御する送信制御ステップと、コンテンツを再生するために必要な第5の情報の受信を制御する受信制御ステップと、受信制御ステップの処理により受信が制御された第5の情報に添付されている第6の情報を抽出する抽出ステップと、抽出ステップの処理により抽出された第6の情報を、コンテンツに添付されている第1の情報に代わって、コンテンツに添付させる情報添付ステップと

を含む処理をコンピュータに実行させることを特徴とする。

【0018】本発明の第2の情報処理装置は、コンテンツを取得する取得手段と、コンテンツに添付されている第1の情報、コンテンツを特定するための第2の情報、および自分自身を特定することができる第3の情報を含む第4の情報を生成する生成手段と、生成手段により生成された第4の情報を送信する送信手段と、コンテンツを再生するために必要な第5の情報の受信する受信手段と、自分自身を特定することができる第6の情報を、第4の情報の送信先の公開鍵で暗号化する暗号化手段と、暗号化手段により暗号化された第6の情報を、コンテンツに添付されている第1の情報に代わって、コンテンツに添付させる情報添付手段とを備えることを特徴とする。

【0019】本発明の第2の情報処理方法は、コンテンツの取得を制御する取得制御ステップと、コンテンツに添付されている第1の情報、コンテンツを特定するための第2の情報、および自分自身を特定することができる第3の情報を含む第4の情報を生成する生成ステップと、生成ステップの処理により生成された第4の情報の送信を制御する送信制御ステップと、コンテンツを再生するために必要な第5の情報の受信を制御する受信制御ステップと、自分自身を特定することができる第6の情報を、第4の情報の送信先の公開鍵で暗号化する暗号化ステップと、暗号化ステップの処理により暗号化された第6の情報を、コンテンツに添付されている第1の情報に代わって、コンテンツに添付させる情報添付ステップとを含むことを特徴とする。

【0020】本発明の第2の記録媒体に記録されているプログラムは、コンテンツの取得を制御する取得制御ステップと、コンテンツに添付されている第1の情報、コンテンツを特定するための第2の情報、および自分自身を特定することができる第3の情報を含む第4の情報を生成する生成ステップと、生成ステップの処理により生成された第4の情報の送信を制御する送信制御ステップと、コンテンツを再生するために必要な第5の情報の受信を制御する受信制御ステップと、自分自身を特定することができる第6の情報を、第4の情報の送信先の公開鍵で暗号化する暗号化ステップと、暗号化ステップの処理により暗号化された第6の情報を、コンテンツに添付されている第1の情報に代わって、コンテンツに添付させる情報添付ステップとを含むことを特徴とする。

【0021】本発明の第2のプログラムは、コンテンツの取得を制御する取得制御ステップと、コンテンツに添付されている第1の情報、コンテンツを特定するための第2の情報、および自分自身を特定することができる第3の情報を含む第4の情報を生成する生成ステップと、生成ステップの処理により生成された第4の情報の送信を制御する送信制御ステップと、コンテンツを再生する

ために必要な第5の情報の受信を制御する受信制御ステップと、自分自身を特定することができる第6の情報を、第4の情報の送信先の公開鍵で暗号化する暗号化ステップと、暗号化ステップの処理により暗号化された第6の情報を、コンテンツに添付されている第1の情報に代わって、コンテンツに添付させる情報添付ステップとを含む処理をコンピュータに実行させることを特徴とする。

【0022】本発明の第3の情報処理装置は、コンテンツを再生させるために用いられる、コンテンツに固有の第1の情報を記録する第1の記録手段と、コンテンツを保有する他の情報処理装置から、コンテンツに添付されている第2の情報、コンテンツを特定するための第3の情報、および、他の情報処理装置を特定するための第4の情報を含む第5の情報の受信する受信手段と、第1の記録手段に記録されている第1の情報のうち、第3の情報によって特定されるコンテンツに対応する第1の情報を抽出する抽出手段と、他の情報処理装置を特定する情報を少なくとも含む第6の情報を生成する第1の生成手段と、第1の生成手段により生成された第6の情報、および抽出手段により抽出された第1の情報を少なくとも含む第7の情報を生成する第2の生成手段と、第2の生成手段により生成された第7の情報を第4の情報により特定される他の情報処理装置へ送信する送信手段とを備えることを特徴とする。

【0023】第1の生成手段により生成された第6の情報を、自分自身の公開鍵で暗号化する暗号化手段を更に備えるようにすることができ、第2の生成手段には、暗号化手段により暗号化された第6の情報、および抽出手段により抽出された第1の情報を少なくとも含む第7の情報を生成させるようにすることができる。

【0024】受信手段により受信された第5の情報に含まれている第2の情報を自分自身の秘密鍵を用いて復号する復号手段を更に備えさせるようにことができ、第2の情報は、公開鍵により暗号化されている情報であるものとしてすることができる。

【0025】第1の情報は、コンテンツを条件付で再生させるための第1のライセンス情報と、コンテンツを完全に再生させるための第2のライセンス情報のいずれかであるものとしてすることができる。

【0026】第2の生成手段により生成された第7の情報を暗号化する暗号化手段を更に備えさせるようにすることができる。

【0027】暗号化手段には、第7の情報を、第4の情報により特定される他の情報処理装置の公開鍵で暗号化させ、自分自身の秘密鍵で電子署名を施させるようにすることができる。

【0028】受信手段により受信された第5の情報を復号する復号手段を更に備えさせるようにすることができる。

【0029】受信手段により受信された第5の情報に含まれている、第2の情報、第3の情報、および第4の情報を記録する第2の記録手段と、第2の記録手段により記録された第2の情報、第3の情報、および第4の情報を基に、コンテンツに関する情報を解析する解析手段を更に備えさせるようにすることができる。

【0030】本発明の第3の情報処理方法は、コンテンツを再生させるために用いられる、コンテンツに固有の第1の情報の記録を制御する記録制御ステップと、コンテンツを保有する他の情報処理装置からの、コンテンツに添付されている第2の情報、コンテンツを特定するための第3の情報、および、他の情報処理装置を特定するための第4の情報を含む第5の情報の受信を制御する受信制御ステップと、記録制御ステップの処理により記録が制御されている第1の情報のうち、第3の情報によって特定されるコンテンツに対応する第1の情報を抽出する抽出ステップと、他の情報処理装置を特定する情報を少なくとも含む第6の情報を生成する第1の生成ステップと、第1の生成ステップの処理により生成された第6の情報、および抽出ステップの処理により抽出された第1の情報を少なくとも含む第7の情報を生成する第2の生成ステップと、第2の生成ステップの処理により生成された第7の情報の、第4の情報により特定される他の情報処理装置への送信を制御する送信制御ステップとを含むことを特徴とする。

【0031】本発明の第3の記録媒体に記録されているプログラムは、コンテンツを再生させるために用いられる、コンテンツに固有の第1の情報の記録を制御する記録制御ステップと、コンテンツを保有する他の情報処理装置からの、コンテンツに添付されている第2の情報、コンテンツを特定するための第3の情報、および、他の情報処理装置を特定するための第4の情報を含む第5の情報の受信を制御する受信制御ステップと、記録制御ステップの処理により記録が制御されている第1の情報のうち、第3の情報によって特定されるコンテンツに対応する第1の情報を抽出する抽出ステップと、他の情報処理装置を特定する情報を少なくとも含む第6の情報を生成する第1の生成ステップと、第1の生成ステップの処理により生成された第6の情報、および抽出ステップの処理により抽出された第1の情報を少なくとも含む第7の情報を生成する第2の生成ステップと、第2の生成ステップの処理により生成された第7の情報の、第4の情報により特定される他の情報処理装置への送信を制御する送信制御ステップとを含むことを特徴とする。

【0032】本発明の第3のプログラムは、コンテンツを再生させるために用いられる、コンテンツに固有の第1の情報の記録を制御する記録制御ステップと、コンテンツを保有する他の情報処理装置からの、コンテンツに添付されている第2の情報、コンテンツを特定するための第3の情報、および、他の情報処理装置を特定するた

めの第 4 の情報を含む第 5 の情報の受信を制御する受信制御ステップと、記録制御ステップの処理により記録が制御されている第 1 の情報のうち、第 3 の情報によって特定されるコンテンツに対応する第 1 の情報を抽出する抽出ステップと、他の情報処理装置を特定する情報を少なくとも含む第 6 の情報を生成する第 1 の生成ステップと、第 1 の生成ステップの処理により生成された第 6 の情報、および抽出ステップの処理により抽出された第 1 の情報を少なくとも含む第 7 の情報を生成する第 2 の生成ステップと、第 2 の生成ステップの処理により生成された第 7 の情報の、第 4 の情報により特定される他の情報処理装置への送信を制御する送信制御ステップとを含む処理をコンピュータに実行させることを特徴とする。

【 0 0 3 3 】本発明の情報処理システムは、第 1 の情報処理装置が、コンテンツを取得する取得手段と、コンテンツに添付されている第 1 の情報、コンテンツを特定するための第 2 の情報、および自分自身を特定することができる第 3 の情報を含む第 4 の情報を生成する第 1 の生成手段と、第 1 の生成手段により生成された第 4 の情報を第 2 の情報処理装置へ送信する第 1 の送信手段と、第 2 の情報処理装置から送信されたコンテンツを再生するために必要な第 5 の情報を受信する第 1 の受信手段と、受信手段により受信された第 5 の情報に添付されている第 6 の情報を抽出する第 1 の抽出手段と、第 1 の抽出手段により抽出された第 6 の情報を、コンテンツに添付されている第 1 の情報に代わって、コンテンツに添付させる情報添付手段とを備え、第 2 の情報処理装置が、コンテンツを再生させるために用いられる、コンテンツに固有の第 7 の情報を記録する記録手段と、第 1 の情報処理装置から、第 1 の情報、第 2 の情報、および、第 3 の情報を含む第 4 の情報を受信する第 2 の受信手段と、記録手段に記録されている第 7 の情報のうち、第 2 の情報によって特定されるコンテンツに対応する第 7 の情報を抽出する第 2 の抽出手段と、第 1 の情報処理装置を特定する情報を少なくとも含む第 6 の情報を生成する第 2 の生成手段と、第 2 の生成手段により生成された第 6 の情報、および第 2 の抽出手段により抽出された第 7 の情報を少なくとも含む第 5 の情報を生成する第 3 の生成手段と、第 3 の生成手段により生成された第 5 の情報を第 3 の情報により特定される第 1 の情報処理装置へ送信する第 2 の送信手段とを備えることを特徴とする。

【 0 0 3 4 】本発明の第 1 の情報処理装置および情報処理方法、並びにプログラムにおいては、コンテンツが取得され、コンテンツに添付されている第 1 の情報、コンテンツを特定するための第 2 の情報、および自分自身を特定することができる第 3 の情報を含む第 4 の情報が生成され、生成された第 4 の情報が送信され、コンテンツを再生するために必要な第 5 の情報が受信され、第 5 の情報に添付されている第 6 の情報が抽出され、抽出された第 6 の情報が、コンテンツに添付されている第 1 の情

報に代わって、コンテンツに添付される。

【 0 0 3 5 】本発明の第 2 の情報処理装置および情報処理方法、並びにプログラムにおいては、コンテンツが取得され、コンテンツに添付されている第 1 の情報、コンテンツを特定するための第 2 の情報、および自分自身を特定することができる第 3 の情報を含む第 4 の情報が生成され、生成された第 4 の情報が送信され、コンテンツを再生するために必要な第 5 の情報が受信され、自分自身を特定することができる第 6 の情報が、第 4 の情報の送信先の公開鍵で暗号化され、暗号化された第 6 の情報が、コンテンツに添付されている第 1 の情報に代わって、コンテンツに添付される。

【 0 0 3 6 】本発明の第 3 の情報処理装置および情報処理方法、並びにプログラムにおいては、コンテンツを再生させるために用いられる、コンテンツに固有の第 1 の情報が記録され、コンテンツを保有する他の情報処理装置から、コンテンツに添付されている第 2 の情報、コンテンツを特定するための第 3 の情報、および、他の情報処理装置を特定するための第 4 の情報を含む第 5 の情報が受信され、記録されている第 1 の情報のうち、第 3 の情報によって特定されるコンテンツに対応する第 1 の情報が抽出され、他の情報処理装置を特定する情報を少なくとも含む第 6 の情報が生成され、生成された第 6 の情報、抽出された第 1 の情報を少なくとも含む第 7 の情報が生成され、生成された第 7 の情報が、第 4 の情報により特定される他の情報処理装置へ送信される。

【 0 0 3 7 】本発明の情報処理システムにおいては、第 1 の情報処理装置で、コンテンツが取得され、コンテンツに添付されている第 1 の情報、コンテンツを特定するための第 2 の情報、および自分自身を特定することができる第 3 の情報を含む第 4 の情報が生成され、生成された第 4 の情報が第 2 の情報処理装置へ送信され、第 2 の情報処理装置から送信されたコンテンツを再生するために必要な第 5 の情報が受信され、第 5 の情報に添付されている第 6 の情報が抽出され、抽出された第 6 の情報が、コンテンツに添付されている第 1 の情報に代わって、コンテンツに添付され、第 2 の情報処理装置で、コンテンツを再生させるために用いられる、コンテンツに固有の第 7 の情報が記録され、第 1 の情報処理装置から、第 1 の情報、第 2 の情報、および、第 3 の情報を含む第 4 の情報が受信され、記録されている第 7 の情報のうち、第 2 の情報によって特定されるコンテンツに対応する第 7 の情報が抽出され、第 1 の情報処理装置を特定する情報を少なくとも含む第 6 の情報が生成され、生成された第 6 の情報、および抽出された第 7 の情報を少なくとも含む第 5 の情報が生成され、生成された第 5 の情報が第 3 の情報により特定される第 1 の情報処理装置へ送信される。

【 0 0 3 8 】

【発明の実施の形態】以下、図を参照して、本発明の実

10

20

30

40

50

施の形態について説明する。

【0039】図1は、本発明を適応したコンテンツ配信サービスを提供するために利用されるネットワーク構成図である。

【0040】ユーザが保有するパーソナルコンピュータ1-1乃至1-nは、インターネット2を介して、ライセンスサーバ3、コンテンツサーバ4、および決済サーバ5と接続されている。

【0041】パーソナルコンピュータ1-1乃至1-nは、インターネット2を介して、コンテンツサーバ4から、コンテンツを受信（ダウンロード）する。コンテンツデータには、例えば、楽曲データ、画像データ、静止画像データ、動画データ、あるいは、動画データと音声データとによる映像データなど、様々な形態のものがある。

【0042】コンテンツサーバ4は、パーソナルコンピュータ1-1乃至1-nを利用するユーザが所望するコンテンツデータを、コンテンツデータベース13から検索して、インターネット2を介して、パーソナルコンピュータ1-1乃至1-nに送信する。コンテンツデータベース13に記録されているコンテンツデータは、暗号化されている。コンテンツサーバ4は、例えば、インターネット2上に、コンテンツのダウンロードを行うことができるウェブサイト（ダウンロードサイト）を公開するようにしても良い。

【0043】図2を用いて、コンテンツデータベース13にコンテンツデータとともに登録されているコンテンツ管理テーブルについて説明する。

【0044】コンテンツ管理テーブルには、コンテンツを表す固有のIDであるコンテンツID、コンテンツを記録している場所を示すアドレス情報、および対応するコンテンツを再生する場合に利用されるライセンスIDなどが記録されている。ライセンスIDは、通常ライセンス用のライセンスIDと、プレビューライセンス用のライセンスIDが登録されている。コンテンツサーバ4はライセンスを発行せず、コンテンツデータベース13も、コンテンツに対するライセンスを保存しているわけではないので、コンテンツ管理テーブルでは、ライセンスIDを必ずしも登録する必要はない。しかしながら、ライセンスに含まれるコンテンツを復号するための復号鍵（ライセンスキー）は、コンテンツサーバ4が、それぞれのコンテンツを暗号化した暗号化鍵と一対を成す鍵であるので、コンテンツ管理テーブルにおいて、ライセンスIDとコンテンツIDとの関係が管理されているほうが望ましい。

【0045】ここで、通常ライセンスとは、コンテンツを完全に再生することが出来るライセンスであり、プレビューライセンスとは、その内容の一部を確認するための、いわゆるお試し再生（例えば、コンテンツの一部の再生など）ができるライセンスである。

【0046】また、パーソナルコンピュータ1-1乃至パーソナルコンピュータ1-nは、コンテンツサーバ4から受信したコンテンツデータを、自分自身以外のパーソナルコンピュータ1-1乃至パーソナルコンピュータ1-nと、ピアツーピアで送受信することが可能である。更に、他のパーソナルコンピュータから受信したコンテンツデータを、他のパーソナルコンピュータにピアツーピアで同様にして送信することができるのは言うまでもない。

【0047】このようにして流通されるコンテンツデータは、暗号化されており、コンテンツデータを受信するだけでは、再生して、視聴することができない。そこで、パーソナルコンピュータ1-1乃至1-nは、インターネット2を介して、ライセンスサーバ3に、コンテンツデータを再生するためのライセンスの送信を要求する。

【0048】パーソナルコンピュータ1-1乃至1-nがライセンスサーバ3からライセンスを受信するためには、予め、後述する処理によりユーザ登録を実行する必要がある。ライセンスサーバ3は、パーソナルコンピュータ1-1乃至1-nよりユーザ登録情報の入力を受け、登録されるユーザのそれぞれに固有の番号であるユーザIDを発行する。

【0049】ライセンスサーバ3には、ユーザ登録データベース11およびライセンス情報データベース12が接続されており、ユーザが、パーソナルコンピュータ1-1乃至1-nを用いてコンテンツサーバ4から配信される、あるいは、ピアツーピアで、他のパーソナルコンピュータからコピーしたコンテンツを再生するためのライセンスを発行する。

【0050】ライセンスには、コンテンツデータの全てを復号することが可能な通常ライセンスと、ユーザがコンテンツの内容を確認するための制限的な再生、すなわち、コンテンツの一部のみ、あるいは、ビットレートや解像度が落とされた（いわゆる、デグレードされた）コンテンツを再生することができるプレビューライセンスがある。パーソナルコンピュータ1-1乃至1-nは、通常ライセンス、もしくはプレビューライセンスをライセンスサーバに要求する。

【0051】ライセンスには、通常ライセンスであるかプレビューライセンスであるかを示すライセンスステータス、所定のコンテンツを復号するための復号鍵（ライセンスキー）、必要に応じて、コピーガード情報、コンテンツを再生する場合の制限（例えば、再生可能期間や再生可能回数、あるいは、コピー可能回数など）を示す制限情報、および、コンテンツの流通経路をトレーシングするために用いられるユーザ情報が含まれている。ユーザ情報には、コンテンツの配信元を示すために、例えば、ユーザIDなど、ユーザを特定することができる情報が少なくとも含まれており、ライセンスサーバ3の公

公開鍵で暗号化されている。また、ライセンスには、上述する以外にも、コンテンツに付随する各種情報などを含ませるようにしてもよい。

【0052】決済サーバ5は、通常ライセンス発行に先立って、パーソナルコンピュータ1-1乃至1-nを保有するユーザと、ライセンスサーバ3の管理者との課金処理を実行するものである。課金方法としては、例えば、クレジットカード決済、プリペイドカードを用いた決済、電子マネーによる決済など、いずれの方法を用いるようにしてもよい。

【0053】また、コンテンツサーバ4から配信され、パーソナルコンピュータ1-1乃至1-n間をピアツーピアで授受されるコンテンツデータには、ユーザ情報を記載するためのフィールドが付加されている。

【0054】例えば、コンテンツサーバ4から、コンテンツが配信された場合、そのフィールドには、コンテンツサーバ4から配信されたことを示す情報を含む、コンテンツサーバ4のユーザ情報が記載されている。そして、ユーザAが保有するパーソナルコンピュータ1-1で、対応するコンテンツのライセンスが取得された場合（プレビューでも、通常でもよい）、ライセンスには、ユーザAを特定するための情報を含むユーザ情報が含まれており、そのフィールドに記載されている情報は、ユーザAのユーザ情報に書き換えられる。

【0055】そして、そのコンテンツが、ユーザAが保有するパーソナルコンピュータ1-1からユーザBが保有するパーソナルコンピュータ1-2へピアツーピアで送信される場合、そのフィールドには、コンテンツの配信元となるユーザAのユーザのユーザ情報が記載されている。そして、ユーザBが保有するパーソナルコンピュータ1-2において、ライセンスが取得された場合、ライセンスには、ユーザBのユーザ情報が含まれており、コンテンツに添付されているフィールドに記載されている情報は、ユーザBのユーザ情報に書き換えられる。

【0056】本システムにおいては、ライセンスサーバ3と登録済みのパーソナルコンピュータ1-1乃至1-nとが、インターネット2を介して、安全性の高い情報の授受を行うために、公開鍵暗号方式を利用するものとする。従って、ライセンスサーバ3は、ユーザ登録時に、登録されるユーザの公開鍵を入手するとともに、ライセンスサーバの公開鍵を登録されたユーザが利用しているパーソナルコンピュータ1-1乃至1-nに送信する。

【0057】公開鍵暗号方式とは、データ暗号化方式の1つである。公開鍵暗号方式では、データ送信者のデータの暗号化と、データ受信者のデータの復号とで、それぞれ異なる鍵（ビット列）が使用される（公開鍵暗号方式に対して、秘密鍵暗号方式では、暗号化と復号の双方で同じ鍵を用いる）。

【0058】公開鍵暗号方式においては、「公開鍵」と

「秘密鍵」という2種類の鍵が利用される。このうち秘密鍵は、それを生成したユーザが安全な場所に保管しておき、他人にはいっさい公開しない。一方の公開鍵は、データの送信元となる可能性がある（自分に対してデータを送る可能性がある）相手に広く配布しておく。具体的には、電子メールに添付して相手に送付してもよいし、公開鍵を管理するサービスを行う事業者に預けて、誰でも参照できるようにしてもよい。そしてデータの送信者は、受信先が発行した公開鍵を入手し、受信先の公開鍵で、送信するデータを暗号化する。こうして暗号化されたデータを復号するには、暗号化に使われた公開鍵に対応する秘密鍵が必要である。このため秘密鍵を持たない第三者がデータを傍受したとしても、データを復号することはできない。

【0059】「公開鍵」と「秘密鍵」の鍵ペアを生成するためには、いくつかの方法があるが、Rivest、Shamir、およびAdlemanによって提唱されたRSAアルゴリズムが有名である。RSAでは、数百桁におよぶ巨大な数の素数の積を用いて公開鍵と秘密鍵を生成する。このような素数から生成された一方の値から、他方を導き出すためには、巨大数の素因数分解が必要になる。この巨大数の素因数分解には膨大な計算処理が必要で、現実的な時間内に答えを出すことは不可能である。ここでは、鍵ペアの生成に、RSAアルゴリズムを利用しても、他の方法を利用しても良い。

【0060】また、公開鍵暗号方式における「秘密鍵」は、そのデータの発信者が、間違いなく本人であることを証明する「電子署名」としても利用することができる。上述したように、通常の暗号化では、受信先が発行した公開鍵でデータを暗号化するが、電子署名では、発信元が送信するデータ（通常は、データにハッシュをかけた値）を自分の秘密鍵で暗号化して電子署名とし、データに付加して相手に送る。これを受け取った相手は、その送信元が発行した公開鍵を使って、電子署名の復号を行う。そして、受信したデータ（データのハッシュ値）と、電子署名を復号したデータを比較して、一致すれば、間違いなく本人が発信した情報であり、改竄されていないことが証明される。ここでは、受信先の公開鍵でデータを暗号化し、送信元の電子署名用の秘密鍵で電子署名を施したデータを送受信するものとする。

【0061】ただし、公開鍵暗号方式では、その公開鍵が本当に本人のものであるか否かが照明されていなければならない。そこで、第三者機関が公的に本人認証を行うためのPKI（Public Key Infrastructure）が利用される。

【0062】PKIでは、認証局（CA：Certification Authority）という信頼できる認証機関を設けて、電子署名による「電子証明書」とともに公開鍵を発行して、管理し、データの授受先の正当性（本人であること）を証明する仕組みを提供する。これにより、データ

の盗聴および改ざん、あるいは、なりすましを防止することができる。

【0063】ライセンスサーバ3と登録済みのユーザが保有するパーソナルコンピュータ1-1乃至1-nは、お互いの公開鍵を交換する。そして、ライセンスサーバ3は、登録済みのユーザが保有するパーソナルコンピュータ1-1乃至1-nのうちのいずれかから、暗号化され、署名されたライセンス取得要求情報を受信する。ライセンス取得要求情報には、送信元ユーザ（ライセンス要求元）のユーザID、ライセンスの取得を要求するコンテンツのコンテンツID、および、そのコンテンツに付随しているフィールドに記載されたユーザ情報が添付される。

【0064】ライセンス取得要求情報を受信したライセンスサーバ3は、ライセンス情報データベース12から、ライセンステーブルを参照して、コンテンツIDに対応するライセンスキー（コンテンツに対する復号鍵）を検索し、例えば、ユーザIDなど、ライセンス供給先を特定するための情報を含むユーザ情報を生成して、ライセンスサーバの公開鍵で暗号化し、ライセンスステータス情報、制限情報などを付加して、ライセンスを生成する。ライセンスサーバ3は、ライセンスを暗号化し、電子署名を施した後、インターネット2を介して、ライセンス取得要求情報の送信元に送信する。ライセンステーブルについては後述する。

【0065】そして、ライセンスサーバ3は、ライセンス情報データベース12のライセンス発行テーブルに、ライセンス発行の履歴を記録し、ライセンス取得要求情報に添付されている情報を基に、コンテンツデータがどのようなユーザを経由して流通しているかを示す情報（以下、トレーシング情報と称する）を抽出して、ライセンス情報データベース12のトレーシング情報テーブルに記録する。ライセンス発行テーブル、およびトレーシング情報テーブルについては後述する。

【0066】以下、パーソナルコンピュータ1-1乃至パーソナルコンピュータ1-nを個々に区別する必要がない場合、単にパーソナルコンピュータ1と総称する。

【0067】図3は、パーソナルコンピュータ1の構成を示すブロック図である。

【0068】CPU (Central Processing Unit) 21は、入出力インターフェース22および内部バス23を介して、ユーザが、入力部24を用いて入力した各種指令に対応する信号や、ネットワークインターフェース30を介して、例えば、ライセンスサーバ3などが送信した信号の入力を受け、入力された信号に基づいた各種処理を実行する。ROM (Read Only Memory) 25は、CPU 21が使用するプログラムや演算用のパラメータのうちの基本的に固定のデータを格納する。RAM (Random Access Memory) 26は、CPU 21の実行において使用するプログラムや、その実行において適宜変化する

パラメータを格納する。CPU 21、ROM 25、およびRAM 26は、内部バス23により相互に接続されている。

【0069】内部バス23は、入出力インターフェース22とも接続されている。入力部24は、例えば、キーボード、タッチパッド、ジョグダイヤル、あるいはマウスなどからなり、ユーザがCPU 21に各種の指令を入力するとき操作される。出力部27は、例えば、CRT (Cathode Ray Tube) や液晶表示装置などで構成される。各種情報をテキスト、あるいはイメージなどで表示する表示部や、音声を出力するスピーカ、更に、必要に応じて、音を発生するブザーや、点灯、もしくは消灯によりユーザに情報を伝達するためのLEDランプなどで構成される。

【0070】HDD (hard disk drive) 28は、ハードディスクを駆動し、それらにCPU 21によって実行するプログラムや情報（例えば、コンテンツデータ）を記録または再生させる。ドライブ29には、必要に応じて磁気ディスク31、光ディスク32、光磁気ディスク33、および半導体メモリ34が装着され、データの授受を行う。

【0071】ネットワークインターフェース30は、インターネット2と接続され、インターネット2を介して、ライセンスサーバ3などと情報の授受を行う。また、ネットワークインターフェース30は、例えば、コンテンツデータを記憶している外部の記憶装置と接続されていても良い。

【0072】これらの入力部24乃至ネットワークインターフェース30は、入出力インターフェース22および内部バス23を介してCPU 21に接続されている。

【0073】なお、ライセンスサーバ3乃至決済サーバ5も、基本的に、パーソナルコンピュータ1と同様の構成を有するものであるため、そのハードウェアに関する詳細な説明は省略する。

【0074】図4は、パーソナルコンピュータ1を利用するユーザのユーザ登録を実行し、パーソナルコンピュータ1が記録しているコンテンツデータを再生するための通常ライセンス、もしくはプレビューライセンスを発行するライセンスサーバ3の機能を示す機能ブロック図である。

【0075】制御部41は、インターネット2および入出力インターフェース42を介して入力された、パーソナルコンピュータ1から送信された各種情報を基に、ライセンスサーバ3の動作を制御するものである。制御部41は、例えば、パーソナルコンピュータ1から送信されたユーザの登録情報などをユーザ登録データベース1に登録したり、新たに登録されたユーザが保有するパーソナルコンピュータ1に、メモリ43に記録されている、ライセンスサーバ3の公開鍵や、コンテンツ復号アプリケーションプログラムなどを送信したり、ライセン

ス取得要求を受けて、対応するコンテンツのライセンスを生成し、要求元のパーソナルコンピュータ 1 に送信する処理を制御する。

【0076】入出力インターフェース 42 は、ライセンスサーバ 3 が、ユーザ登録データベース 11、ライセンス情報データベース 12、および、インターネット 2 と情報の授受を行うためのインターフェースである。

【0077】メモリ 43 には、ライセンスサーバ 3 の公開鍵や、コンテンツ復号アプリケーションプログラムなどの、パーソナルコンピュータ 1 に送信される情報や、

制御部 41 の処理に必要な各種情報が記録されている。

【0078】暗号化および復号処理部 44 は、登録済みのユーザが有するパーソナルコンピュータ 1 との通信において、送信する情報を暗号化し、署名するとともに、受信した情報の署名を確認し、復号する処理や、ライセンスに添付するユーザ情報を暗号化したり、ライセンス取得要求情報に含まれているユーザ情報を復号する処理を実行する。また、暗号化および復号処理部 44 は、その内部に、秘密鍵記録部 51 を備え、暗号化および署名の確認に用いられる、ライセンスサーバ 3 の秘密鍵を保存している。

【0079】トレーシングデータ解析部 45 は、ライセンス取得要求情報に添付されているユーザ情報などを基に、ライセンス情報データベース 12 のトレーシング情報テーブルに登録されるデータから、それぞれのコンテンツが、どのような経路でユーザに配信されたのであるかを解析し、解析結果を基に、コンテンツ配信事業に有益な、様々なデータを抽出する。

【0080】次に、図 5 のフローチャートを参照して、ユーザ登録実行時のパーソナルコンピュータ 1 とライセンスサーバ 3 との処理について説明する。

【0081】ステップ S1 において、パーソナルコンピュータ 1 の CPU 21 は、入出力インターフェース 22 および内部バス 23 を介して、入力部 24 から入力されたユーザの操作を示す信号に従って、内部バス 23、入出力インターフェース 22、ネットワークインターフェース 30、およびインターネット 2 を介して、ライセンスサーバ 3 にアクセスする。パーソナルコンピュータ 1 の CPU 21 は、例えば、ウェブブラウザを起動し、ライセンスサーバ 3 が公開しているウェブページにアクセスするようにしても良い。

【0082】ステップ S2 において、パーソナルコンピュータ 1 の CPU 21 は、ユーザ登録情報およびユーザの公開鍵（データ暗号化用および署名復号用）を、ライセンスサーバ 3 に送信する。ここでは、ユーザの公開鍵をライセンスサーバ 3 に送信するものとして説明したが、例えば、公開鍵を一般に公開するような場合は、公開鍵の入手方法についての情報をライセンスサーバ 3 に送信するようにしても良い。

【0083】ステップ S3 において、ライセンスサーバ 50

3 の制御部 41 は、インターネット 2 および入出力インターフェース 42 を介して、ユーザ登録情報およびユーザの公開鍵（もしくは公開鍵の入手方法についての情報）を受信し、新たに登録するユーザのためのユーザ ID を設定する。

【0084】ステップ S4 において、ライセンスサーバ 3 の制御部 41 は、設定されたユーザ ID とともに、ユーザ登録情報およびユーザの公開鍵を、入出力インターフェース 42 を介して、ユーザ登録データベース 11 に登録する。

【0085】ユーザ登録データベース 11 には、図 6 に示されるユーザ登録管理テーブルが登録されている。ユーザ登録管理テーブルには、ライセンスサーバ 3 が発行したユーザ ID 毎に、例えば、上述した公開鍵暗号方式を用いて情報を授受するためのユーザの公開鍵、ライセンスの送信先として登録されるメールアドレスに加えて、必要に応じて、ユーザの個人情報（ユーザの嗜好情報などを含む）などが登録される。

【0086】ステップ S5 において、ライセンスサーバ 3 の制御部 41 は、コンテンツ復号アプリケーションプログラムをメモリ 43 から読み出し、入出力インターフェース 42 およびインターネット 2 を介して、パーソナルコンピュータ 1 に送信する。コンテンツ復号アプリケーションプログラムとは、パーソナルコンピュータ 1 において、ライセンス取得要求情報を生成して送信したり、ライセンス取得時に、コンテンツに付随しているフィールドに記載されているユーザ情報の書き換え処理を実行したり、コンテンツデータを取得したライセンスで復号する処理を実行するアプリケーションであり、その詳細については後述する。

【0087】ステップ S6 において、パーソナルコンピュータ 1 の CPU 21 は、コンテンツ復号アプリケーションプログラムを受信し、インストールする。すなわち、CPU 21 は、コンテンツ復号アプリケーションプログラムを HDD 28 に記録し、CPU 21 の制御に従って、RAM 26 にロードして実行することができるような状態にする。

【0088】ステップ S7 において、ライセンスサーバ 3 の制御部 41 は、ライセンスサーバ 3 の公開鍵（データ暗号化用および署名復号用）、およびステップ S3 において設定されたユーザ ID を、入出力インターフェース 42 およびインターネット 2 を介して、パーソナルコンピュータ 1 に送信する。

【0089】ステップ S8 において、パーソナルコンピュータ 1 の CPU 21 は、ライセンスサーバの公開鍵、およびユーザ ID を受信し、HDD 28 に記録して、処理が終了する。

【0090】以上説明した登録処理により、登録ユーザに対して、ユーザ毎に固有の番号であるユーザ ID が設定されて、ライセンスサーバ 3 およびパーソナルコンピ

ユーザ 1 の両方で記録される。そして、公開鍵暗号方式による情報の授受を行うために、ライセンスサーバ 3 は、自分自身の秘密鍵を保存するとともに、公開鍵を登録済みのユーザに公開（登録済みのユーザが有するパーソナルコンピュータ 1 に送信）し、登録済みのユーザは、自分自身が有するパーソナルコンピュータ 1 に秘密鍵を保存するとともに、公開鍵をライセンスサーバ 3 に公開する。

【0091】また、図 5 においては、ライセンスサーバ 3 が、ユーザ ID を設定するものとして説明しているが、例えば、既にユーザに提供されている他のサービスのユーザ ID や、携帯電話機などの機器に個別に割り当てられている機器 ID などを流用するようにしても、それらの ID がユーザに対して個別に割り当てられてい

ればかまわない。

【0092】図 7 は、図 5 のステップ S 6 で受信し、インストールしたコンテンツ復号アプリケーションプログラムが起動している場合の、パーソナルコンピュータ 1 の機能ブロック図である。

【0093】制御部 61 は、入力部 24 を用いてユーザが行った操作入力に従って、コンテンツ復号アプリケーションプログラムの動作を制御するものである。制御部 61 は、例えば、暗号化および復号処理部 64 の処理により暗号化され、電子署名が記載されたライセンス取得要求情報を、入出力インターフェース 62 およびインターネット 2 を介して、ライセンスサーバ 3 に送信したり、コンテンツサーバ 4 から受信したコンテンツデータを、コンテンツデータベース 66 に保存し、コンテンツ管理テーブル 67 を更新する処理を制御する。

【0094】入出力インターフェース 62 は、パーソナルコンピュータ 1 が、インターネット 2 を介して、ライセンスサーバ 3 乃至決済サーバ 5 と情報の授受を行うためのインターフェースである。

【0095】メモリ 63 は、HDD 28、ROM 25、もしくは RAM 26 に対応する。メモリ 63 には、図 5 のステップ S 8 において記録されたライセンスサーバ 3 の公開鍵および登録時に発行されたユーザ ID、並びに課金処理に必要な個人情報とともに、制御部 61 の処理に必要な各種情報が記録されている。

【0096】暗号化および復号処理部 64 は、ライセンスサーバ 3 との通信において、送信する情報を暗号化し、署名するとともに、受信した情報の署名を確認し、復号する処理や、ライセンスサーバ 3 から配布されたライセンスを用いて、コンテンツデータを復号する処理を実行する。また、暗号化および復号処理部 64 は、その内部に、秘密鍵記録部 71 を備え、暗号化および署名の確認に用いられる、ユーザの秘密鍵を保存している。

【0097】再生処理部 65 は、暗号化および復号処理部 64 で復号されたコンテンツデータの入力を受け、所定のフォーマットに従って、データ伸長処理、エラー訂

正処理、各種画像処理、あるいは音声データの D/A 変換処理などの必要な処理を実行して、画像データは出力部 27 の表示部 72 に、音声データは出力部 27 のスピーカ 73 に、それぞれ出力する。

【0098】コンテンツデータベース 66 は、コンテンツサーバ 4 からダウンロードした、暗号化されたコンテンツデータを記録している。コンテンツ管理テーブル 67 には、ダウンロードしたコンテンツのコンテンツ ID、コンテンツが記録されているアドレス情報、およびライセンスの有無やライセンス ID を記録している図 11 を用いて後述するコンテンツ管理テーブルとともに、ライセンスサーバ 3 から受信したライセンスに含まれるライセンスキーが保存されている。

【0099】次に、図 8 および図 9 のフローチャートを参照して、登録済みのユーザが保有しているパーソナルコンピュータ 1 において、図 7 を用いて説明したコンテンツ復号アプリケーションプログラムが RAM 26 にロードされ、CPU 21 において実行されている場合の処理について説明する。

【0100】ステップ S 21 において、制御部 61 は、インターネット 2 および入出力インターフェース 62 を介して、コンテンツサーバ 4 から、所望のコンテンツをダウンロードし、コンテンツデータベース 66 に保存するとともに、コンテンツ管理テーブル 67 に記録されている情報を更新する。制御部 61 は、例えば、ウェブブラウザを起動し、コンテンツサーバ 4 が公開しているウェブページ（ダウンロードサイト）にアクセスし、所定の操作を実行して、所望のコンテンツデータをダウンロードするようにしても良い。

【0101】コンテンツは暗号化されており、通信経路上で、悪意ある第三者にデータを盗まれるようなことがあっても、対応するライセンスがなければ、コンテンツを再生することは出来ない。従って、コンテンツサーバ 4 とパーソナルコンピュータ 1-1 とのコンテンツデータの送受信は、上述した公開鍵暗号方式を用いずに実行される（図 10 の図中 a）。図 10 においては、インターネット 2 は図示されていないが、情報の授受は、インターネット 2 を介して実行されている。

【0102】また、図 10 の図中 b に示されるように、コンテンツサーバ 4 からダウンロードされるコンテンツデータに添付しているフィールドには、このコンテンツデータがコンテンツサーバ 4 からダウンロードされたデータであることを示すユーザ情報（図中、`con-se-r-ver` と記載されている情報）が記載されている。ユーザ情報は、ライセンスサーバ 3 の公開鍵で暗号化されているので、ライセンスサーバ 3 の暗号化および復号処理部 44 でしか復号されることはない。

【0103】また、ユーザ情報が、ライセンスサーバ 3 の公開鍵で暗号化され、ライセンスサーバ 3 においてのみ読み取りが可能であることを利用して、ユーザ情報

10

20

30

40

50

に、例えば、ライセンスの発行日時を示す情報や、コンテンツおよびライセンスの発行サービスに関する情報を付加することも可能である。

【0104】そして、制御部61は、コンテンツ管理テーブル67を用いて、ダウンロードされて、コンテンツデータベース66に記録されている、暗号化されたコンテンツデータおよびそれぞれのコンテンツに対応するライセンスを管理する。

【0105】図11を用いて、コンテンツ管理テーブル67に登録される情報について説明する。コンテンツ管理テーブル67には、コンテンツデータベース66に保存されているコンテンツを表す固有のIDであるコンテンツID、コンテンツデータベース66内で、コンテンツを記録している場所を示すアドレス情報、および対応するコンテンツを再生する場合に利用される、通常ライセンス用のライセンスIDと、プレビューライセンス用のライセンスIDが登録されている。ライセンスの発行要求をまだ行っていないコンテンツについては、もちろん、ライセンスIDは登録されておらず、コンテンツによっては、通常ライセンス用のライセンスIDと、プレビューライセンス用のライセンスIDのいずれか一方のみが登録されている場合もある。

【0106】ステップS22において、制御部61は、入力部24から入力されるユーザの操作を示す信号を基に、ユーザから、プレビュー再生用のライセンス取得を指令する入力を受けたか否かを判断する。ステップS22において、プレビュー再生用のライセンス取得を指令する入力を受けていないと判断された場合、処理は、ステップS27に進む。

【0107】ステップS22において、プレビュー再生用のライセンス取得を指令する入力を受けたと判断された場合、ステップS23において、制御部61は、対応するコンテンツのコンテンツIDと、自分自身のユーザID、およびそのコンテンツに付加されているユーザ情報（例えば、コンテンツサーバ4を示す情報（`content server`）を含むユーザ情報）を添付したプレビューライセンス取得要求情報を生成する。

【0108】ステップS24において、制御部61は、ステップS23において生成したプレビューライセンス取得要求情報、およびメモリ63に記録されているライセンスサーバ3の公開鍵を、暗号化および復号処理部64に出力する。暗号化および復号処理部64は、プレビューライセンス取得要求情報をライセンスサーバ3の公開鍵で暗号化する。

【0109】ステップS25において、暗号化および復号処理部64は、秘密鍵記録部71に記録されている自分自身の署名用の秘密鍵を用いて、プレビューライセンス取得要求情報に電子署名を施す。

【0110】ステップS26において、制御部61は、暗号化および復号処理部64によって暗号化され、電子

署名されたプレビューライセンス取得要求情報を、図10の図中cに示されるように、インターネット2を介して、ライセンスサーバ3に送信する。ライセンスサーバ3に送信されるプレビューライセンス取得要求情報には、図10の図中dに示されるように、このコンテンツデータがコンテンツサーバ4からダウンロードされたデータであることを示すユーザ情報（図中、`content server`と記載されている情報）、自分自身のユーザID（図中、`a1111111`と記載されている情報）、およびコンテンツID（図中、`xxxx`と記載されている情報）が、少なくとも記載されている。

【0111】ここで、ライセンスサーバ3は、プレビューライセンス発行のための条件が満たされているか否かを判断し、条件が満たされている場合、プレビューライセンスを発行する（後述する図15および図16のステップS66乃至ステップS68、およびステップS73乃至ステップS76の処理）。

【0112】ステップS22において、プレビュー再生用のライセンス取得を指令する入力を受けていないと判断された場合、ステップS27において、制御部61は、入力部24から入力されるユーザの操作を示す信号を基に、ユーザから、通常再生用のライセンス取得を指令する入力を受けたか否かを判断する。ステップS27において、通常再生用のライセンス取得を指令する入力を受けていないと判断された場合、処理は、ステップS22に戻り、それ以降の処理が繰り返される。

【0113】ステップS27において、通常再生用のライセンス取得を指令する入力を受けたと判断された場合、ステップS28において、制御部61は、対応するコンテンツのコンテンツID、自分自身のユーザID、および、そのコンテンツに付加されているユーザ情報を添付した通常ライセンス取得要求情報を生成する。

【0114】ステップS29において、制御部61は、ステップS28において生成した通常ライセンス取得要求情報、およびメモリ63に記録されているライセンスサーバ3の公開鍵を、暗号化および復号処理部64に出力する。暗号化および復号処理部64は、通常ライセンス取得要求情報をライセンスサーバ3の公開鍵で暗号化する。

【0115】ステップS30において、暗号化および復号処理部64は、秘密鍵記録部71に記録されている自分自身の署名用の秘密鍵を用いて、通常ライセンス取得要求情報に電子署名を施す。

【0116】ステップS31において、制御部61は、暗号化および復号処理部64によって暗号化され、電子署名された通常ライセンス取得要求情報を、ステップS26において説明した場合と同様に、図10の図中cに示されるように、インターネット2を介して、ライセンスサーバ3に送信する。ライセンスサーバ3に送信されるプレビューライセンス取得要求情報にも、ステップS

26において説明した場合と同様に、図10の図中dに示されるように、このコンテンツデータがコンテンツサーバ4からダウンロードされたデータであることを示すユーザ情報が記載されている。

【0117】ここで、ライセンスサーバ3は、課金処理に関する指示を、パーソナルコンピュータ1および決済サーバ5に送信する（後述する図16のステップS69の処理）。

【0118】ステップS32において、制御部61は、図12の図中eに示されるように、課金処理に関する指示を、インターネット2および入出力インターフェース62を介して、ライセンスサーバ5から受信する。ここで、課金処理に関する指示を示す情報は、必要に応じて、ライセンスと同様に、ユーザの公開鍵で暗号化され、ライセンスサーバ3の秘密鍵で署名されていても良いし、他の方法を用いて、情報が安全に送信されるようにしても良い。

【0119】ステップS33において、制御部61は、必要に応じて、暗号化および復号処理部64の処理により、受信した情報の署名を確認し、復号した後、課金処理に関する指示に従って、図12の図中fに示されるように、決済サーバ5にアクセスし、課金処理を実行する。

【0120】ここで、決済サーバ5は、ユーザとの課金処理が正しく実行された場合、ライセンスサーバ3に通常ライセンスの発行リクエストを通知する。そして、ライセンスサーバ3は、課金処理をはじめとする通常ライセンス発行のための条件が満たされているか否かを判断し、条件が満たされている場合、通常ライセンスを発行する（後述する図16のステップS70乃至ステップS76の処理）。

【0121】ステップS26の処理の終了後、もしくは、ステップS33の処理の終了後、ステップS34において、制御部61は、図13の図中hに示されるように、ライセンスサーバ3の署名用の秘密鍵で電子署名され、ユーザの公開鍵で暗号化されたデータ（すなわち、ライセンス）を、インターネット2および入出力インターフェース62を介して、ライセンスサーバ3から受信する。

【0122】ライセンスには、図13の図中gで示されるように、ライセンスが通常ライセンスであるか、プレビューライセンスであるかを示すライセンスステータス、コンテンツを復号するためのライセンスキー、再生回数や、再生時間などの制限情報、およびライセンスサーバの公開鍵で暗号化されているユーザ情報が含まれている。ライセンスに含まれているユーザ情報には、ライセンスを受けるユーザを示す情報（例えば、そのユーザのユーザIDなど）が含まれている。

【0123】このユーザ情報は、コンテンツとともに、ピアツーピアで授受される情報であるので、第三者にユ

ーザを示す情報を盗まれないように、ライセンスサーバの公開鍵で暗号化されているが、ユーザ情報が、例えば、ユーザIDのみで構成されている場合には、暗号化されたデータが毎回同じ値となってしまう。そのため、ユーザIDなどのユーザを特定するための情報以外に、例えば、日時や、サービスに関する情報などの他の情報をユーザ情報に含ませることにより、暗号化されたユーザ情報の値をライセンス毎に変更し、ユーザ情報を第三者に悪用されることを防ぐことが可能である。

【0124】ステップS35において、暗号化および復号処理部64は、受信したデータに対して、メモリ63に保存されているライセンスサーバ3の署名用の公開鍵を用いて署名を確認する。

【0125】ステップS36において、制御部61は、暗号化および復号処理部64が実行した署名を確認する処理の結果を受け、受信したデータの送信元は、間違いなくライセンスサーバ3であるか否かを判断する。

【0126】ステップS36において、受信したデータの送信元はライセンスサーバ3であると判断された場合、ステップS37において、制御部61は、暗号化および復号処理部64を制御して、秘密鍵記録部71に記録されているユーザの秘密鍵で、受信したデータを復号させる。

【0127】ステップS38において、制御部61は、ステップS37において、暗号化および復号処理部64は、受信したデータを正しく復号できたか否かを判断する。

【0128】ステップS36において、受信したデータの送信元はライセンスサーバ3ではないと判断された場合、もしくは、ステップS38において、受信したデータを正しく復号できなかったと判断された場合、ステップS39において、制御部61は、出力部27の表示部72に、エラーメッセージを表示して、処理が終了する。

【0129】ステップS38において、受信したデータを正しく復号できたと判断された場合、ステップS40において、制御部61は、復号したライセンスに含まれるユーザ情報を抽出し、図13の図中iに示されるように、対応するコンテンツのユーザ情報と書き換える（上書きする）。従って、ライセンス取得済みのコンテンツに添付されているフィールドに記載されているユーザ情報は、自分自身を示す情報（例えば、ユーザID）を含むユーザ情報となる。

【0130】ステップS41において、制御部61は、復号されたライセンス（通常ライセンス、もしくはプレビューライセンス）をコンテンツ管理テーブル67に保存する。そして、制御部61は、入力部24から入力されるユーザの操作に従って、必要に応じて、暗号化および復号処理部64に、コンテンツ管理テーブル67に保存されているライセンスのライセンスキーを用いてコン

10

20

30

40

50

テンツを復号させ、再生処理部 65 を制御して、復号されたコンテンツを再生させる。再生されたコンテンツのうち、画像データは、出力部 27 の表示部 72 に出力されて表示され、音声データは、出力部 27 のスピーカ 27 に出力され、音声出力される。

【0131】ここで、ダウンロードされたコンテンツデータは、暗号化された状態でコンテンツデータベース 66 に保存される。すなわち、ライセンスキーで復号されたコンテンツを記録しておくことができないため、再生処理のたびに、ライセンスキーを用いて復号処理が実行される。これにより、ライセンスに、再生回数の制限が含まれている場合、不当な回数の再生処理を未然に防ぐことができる。

【0132】コンテンツの再生回数が制限されている場合、所定の回数を再生したユーザは、新たに、通常ライセンスをライセンスサーバ 3 に要求して、対応するコンテンツを再生する。この場合、もちろん、コンテンツデータを再ダウンロードする必要はないので、コンテンツデータ自身に再生回数の規制がなされて配信される場合と比較して、ユーザは、コンテンツデータのダウンロードのためにインターネット 2 に接続する時間を少なくすることができる。そして、コンテンツ配信サービス事業者は、ライセンスの再供給により、不当な回数の再生処理を未然に防ぎつつ、コンテンツデータの配信に対して、正当な報酬を得ることができる。

【0133】次に、ステップ S42 において、制御部 61 は、他のパーソナルコンピュータから、ピアツーピアでのコンテンツデータのコピーを要求されたか否かを判断する。例えば、図 13 のパーソナルコンピュータ 1-1 は、図 13 の図中 j に示されるように、ライセンスサーバに登録済みであるパーソナルコンピュータ 1-2 からコンテンツデータのコピーを要求されたか否かを判断する。

【0134】ステップ S42 において、他のパーソナルコンピュータから、ピアツーピアでのコンテンツデータのコピーを要求されたと判断された場合、ステップ S43 において、制御部 61 は、自分自身を示すユーザ情報が付加されたコンテンツデータを、図中 k に示されるように、要求元のパーソナルコンピュータに送信して、処理が終了される。ステップ S42 において、他のパーソナルコンピュータ 1 から、ピアツーピアでのコンテンツデータのコピーを要求されていないと判断された場合、処理が終了される。

【0135】パーソナルコンピュータ 1-2 は、パーソナルコンピュータ 1-1 のユーザ情報が付加されたコンテンツデータ（図 13 の図中 i に示されるコンテンツデータ）を受信する。その後、パーソナルコンピュータ 1-2 は、図 14 の図中 l に示されるように、コンテンツ ID、自分自身のユーザ ID、および、パーソナルコンピュータ 1-1 のユーザ情報が付加されたライセンス取

得要求情報を、ライセンスサーバ 3 の公開鍵で暗号化し、パーソナルコンピュータ 1-2 を保有しているユーザの署名用の秘密鍵で署名して、ライセンスサーバ 3 に送信することができる（図 14 の図中 m）。

【0136】ライセンスサーバ 3 は、上述した所定の処理を実行し、パーソナルコンピュータ 1-2 を保有しているユーザの公開鍵で暗号化し、ライセンスサーバ 3 の署名用の秘密鍵で署名したライセンスを、パーソナルコンピュータ 1-2 に送信する（図 14 の図中 n）。このライセンスには、図中 o に示されるように、ライセンスステータス、ライセンスキー、制限情報、およびパーソナルコンピュータ 1-2 を保有しているユーザを示す情報（例えば、ユーザ ID など）を含むユーザ情報を含んでいる。ライセンスを受信したパーソナルコンピュータ 1-2 は、自分自身に保存されているコンテンツデータに付加されているフィールドに記載されているユーザ情報を、受信したライセンスに含まれていた自分自身のユーザ情報に書き換える（図 14 の図中 p）。

【0137】なお、パーソナルコンピュータ 1 を利用するユーザが、決済サーバ 5 に対して、図 5 を用いて説明したライセンスサーバ 3 への登録処理と同様の処理を実行して登録処理を行うようにし、決済サーバ 5 と、パーソナルコンピュータ 1 とが、暗号化された情報をやり取りするようにしても良いことはもちろんである。

【0138】図 8 および図 9 を用いて説明した処理においては、ステップ S33 において、決済サーバ 5 とパーソナルコンピュータ 1 とで実行される課金処理を、ライセンスサーバ 3 に対する通常ライセンス取得要求やライセンスの送受信と独立して実行されるものとして説明したが、例えば、パーソナルコンピュータ 1 からライセンスサーバ 3 へ、通常ライセンス取得要求情報を送信する代わりに、パーソナルコンピュータ 1 は、通常ライセンス取得要求情報を決済サーバ 5 に送信し、決済サーバ 5 が、課金処理の終了後、通常ライセンス取得要求情報を、課金処理を実行したユーザのユーザ ID とともに、ライセンスサーバ 3 に送信するようにしてもよい。この場合、ライセンスサーバ 3 は、決済サーバ 5 から送信された通常ライセンス取得要求情報以外は受理しないものとすることができる。

【0139】次に、図 15 および図 16 を参照して、図 8 および図 9 を用いて説明したパーソナルコンピュータ 1 の処理と並行して実行されるライセンスサーバ 3 の処理について説明する。ここでは、ユーザ情報に含まれる、ユーザを特定するための情報は、ユーザ ID であるものとして説明する。

【0140】ステップ S61 において、ライセンスサーバ 3 の制御部 41 は、パーソナルコンピュータ 1 を有するユーザの秘密鍵で電子署名され、ライセンスサーバ 3 の公開鍵で暗号化されたデータ（図 10 の図中 c、もしくは図 14 の図中 m で示されるデータ）を、インターネ

ット2および入出力インターフェース42を介して受信する。

【0141】ステップS62において、制御部41は、例えば、データの送信者のアドレスなどを検索キーとして、ユーザ登録データベース11に登録されているユーザの公開鍵を検索し、暗号化および復号処理部44にステップS61において受信したデータとともに供給して、検索されたユーザの署名用の公開鍵で電子署名を確認する。

【0142】ステップS63において、制御部41は、ステップS62において復号処理が実行できたか否かを基に、受信したデータの送信元は、登録されているユーザのパーソナルコンピュータ1であるか否かを判断する。

【0143】ステップS63において、受信したデータの送信元は、登録されているユーザのパーソナルコンピュータ1ではないと判断された場合、処理は、後述するステップS78に進む。

【0144】ステップS63において、受信したデータの送信元は、登録されているユーザのパーソナルコンピュータ1であると判断された場合、ステップS64において、制御部41は、暗号化および復号処理部44に、秘密鍵記録部51に記録されているライセンスサーバ3の秘密鍵を用いて、受信したデータを復号させる。

【0145】ステップS65において、制御部41は、ステップS64において復号された受信データは、プレビューライセンス取得要求情報であるか否かを判断する。ステップS65において、受信データは、プレビューライセンス取得要求情報ではないと判断された場合、処理は、後述するステップS69に進む。

【0146】ステップS65において、受信データは、プレビューライセンス取得要求情報であると判断された場合、ステップS66において、制御部41は、プレビューライセンス発行のための条件が満たされているか否かを判断する。例えば、制御部41は、復号されたプレビューライセンス取得要求情報と、ユーザ登録データベース11の登録内容に不一致点がないか（例えば、パスワードを必要としている場合に、パスワードが誤って記載されていないか、など）を確認したり、プレビューライセンスの発行が、1つのコンテンツに1回だけ、もしくは所定の回数以下であると決められているような場合には、ライセンス情報データベース12を参照して、対応するユーザのプレビューライセンスの発行履歴を確認して、所定回数以上のプレビューライセンス要求であるか否かを確認する。

【0147】ステップS66において、プレビューライセンス発行のための条件が満たされていないと判断された場合、処理は、後述するステップS78に進む。

【0148】ステップS66において、プレビューライセンス発行のための条件が満たされていると判断された

場合、ステップS67において、制御部41は、復号されたプレビューライセンス取得要求情報を基に、ライセンスを要求するコンテンツID、受信したライセンス取得要求情報のライセンス種別、ライセンス取得要求情報に添付されているユーザ情報に含まれるユーザID、およびライセンス要求元のユーザIDなどの、ライセンス要求に関する情報を、ライセンス情報データベース12のトレーシング情報テーブルに登録する。

【0149】図17に、トレーシング情報テーブルを示す。トレーシング情報テーブルには、ライセンス取得要求情報に添付されていたコンテンツID、ライセンスの種別を示すライセンスステータス、ユーザ情報に含まれているユーザID、すなわち、コンテンツの配信元のユーザID、およびライセンス取得要求情報を送信した配信先ユーザIDが登録されている。

【0150】ステップS68において、制御部41は、プレビューライセンスを要求されたコンテンツIDを基に、ライセンス情報データベース12のライセンステーブルを参照して、要求されたコンテンツに対応するプレビュー再生用のライセンスキーを検索し、少なくともライセンス取得要求情報を送信したユーザのユーザIDを含むユーザ情報を生成し、必要に応じて、例えば、再生時間や、デグレードの内容（ビットレートや解像度情報）などの制限情報などを付加して、プレビューライセンスを生成して、処理は、後述するステップS73に進む。

【0151】ライセンステーブルを図18に示す。ライセンステーブルには、コンテンツID毎に、通常ライセンスとプレビューライセンスそれぞれのライセンスIDが記録され、必要に応じて、ライセンス情報データベース12内に対応するライセンスが記録されている記録位置を示すアドレス情報が記録されている。

【0152】ステップS65において、受信データはプレビューライセンス取得要求情報ではないと判断された場合、受信データは、通常ライセンス取得要求情報であるので、ステップS69において、制御部41は、課金処理に関する指示を、入出力インターフェース42およびインターネット2を介して、通常ライセンス要求元であるパーソナルコンピュータ1および決済サーバ5に送信する。

【0153】ステップS70において、制御部41は、決済サーバ5から、対応するユーザIDに対して、指定されたコンテンツIDの通常ライセンスの発行リクエストが出されているか否か、すなわち、ユーザが、決済サーバ5との課金処理を正しく終了したか否かを判断する。

【0154】ステップS70において、決済サーバ5から通常ライセンスの発行リクエストが出されていないと判断された場合、処理は、後述するステップS78に進む。

【0155】ステップS70において、決済サーバ5から通常ライセンスの発行リクエストが出されていると判断された場合、ステップS71において、ステップS67と同様の処理が実行される。

【0156】ステップS72において、制御部41は、通常ライセンスを要求されたコンテンツIDを基に、ライセンス情報データベース12のライセンステーブルを参照して、要求されたコンテンツに対応する通常再生用のライセンスキーを検索し、少なくともライセンス取得要求情報を送信したユーザのユーザIDを含むユーザ情報

を生成し、必要に応じて、例えば、再生回数やコピーガードなどの制限情報などを付加して、発行する通常ライセンスを生成する。

【0157】ステップS68の処理の終了後、もしくは、ステップS72の処理の終了後、ステップS73において、制御部41は、ユーザ登録データベース11から、ライセンス要求元のユーザの公開鍵を検索して読み出し、暗号化および復号処理部44に供給する。

【0158】ステップS74において、制御部41は、暗号化および復号処理部44に生成したライセンス（ステップS68において生成したプレビューライセンス、もしくは、ステップS72において生成した通常ライセンス）を供給し、ステップS73において検索された、対応するユーザの公開鍵で暗号化させる。

【0159】ステップS75において、制御部41は、暗号化および復号処理部44を制御して、暗号化されたライセンスに、秘密鍵記録部51に記録されているライセンスサーバ3の署名用の秘密鍵で電子署名を施させる。

【0160】ステップS76において、制御部41は、ユーザ登録データベース11のユーザ登録管理テーブルに登録されているユーザの電子メールアドレスを参照して、暗号化され、電子署名を施されたライセンスを、入出力インターフェース42およびインターネット2を介して、要求元のパーソナルコンピュータ1に送信する（図13の図中h、もしくは図14の図中nで示されるデータ）。

【0161】ステップS77において、制御部41は、ライセンス情報データベース12のライセンス発行テーブルを更新して、処理が終了される。

【0162】図19にライセンス発行テーブルを示す。ライセンス発行テーブルには、ライセンスを発行したユーザID、ライセンスを発行したコンテンツID、発行したライセンスの種類を示すライセンスステータスが登録される。

【0163】ステップS63において、受信したデータの送信元は、登録されているユーザのパーソナルコンピュータ1ではないと判断された場合、ステップS66において、プレビューライセンス発行のための条件が満たされていないと判断された場合、もしくは、ステップS

70において、決済サーバ5から通常ライセンスの発行リクエストが出されていないと判断された場合、ステップS78において、制御部41は、図示しない表示部にエラーメッセージを表示してライセンスサーバ3の管理者にエラーの発生を通知するとともに、必要に応じて、入出力インターフェース42およびインターネット2を介して、パーソナルコンピュータ1にもエラーメッセージを返信して、処理が終了される。

【0164】以上説明した処理により、プレビューライセンス、もしくは通常ライセンスがライセンスサーバ3から、ユーザが保有するパーソナルコンピュータ1に送信されるので、ユーザは、コンテンツサーバ4、もしくは他のパーソナルコンピュータから受信したコンテンツデータを復号して再生することが可能となる。

【0165】そして、コンテンツは、ユーザ情報が添付された状態で、パーソナルコンピュータ1に授受される。ユーザ情報は、ライセンスサーバ3の公開鍵で暗号化されているので、ライセンスサーバ3のみ読み取ることができるようにされている。すなわち、ユーザIDなどを含むユーザ情報がコンテンツとともにピアツーピアで授受されて、悪意ある第三者に傍受された場合においても、悪用されることを防ぐことができる。

【0166】ユーザ情報は、ライセンス取得要求情報に含まれて、パーソナルコンピュータ1からライセンスサーバ3に送信される。パーソナルコンピュータ1は、ライセンスに含まれるユーザ情報を用いて、コンテンツに添付されているユーザ情報を上書きする。ライセンスサーバ3は、ライセンス取得要求情報に含まれるユーザ情報を基に、図17を用いて説明したトレーシング情報テーブルや、図19を用いて説明したライセンス発行テーブルを更新するので、図4を用いて説明したトレーシング情報解析部45の処理により、コンテンツデータの流れをトレーシングすることが可能となる。

【0167】トレーシング情報解析部45は、例えば、図17を用いて説明したトレーシング情報テーブルを基に、コンテンツを他のユーザにピアツーピアで配信したユーザ（配信元ユーザ）に対して、例えば、ポイントなどを発行して、一定のポイントでプレゼントを贈ったり、通常ライセンス購入時にポイント分の料金を割引するなどのサービスを提供することが出来る。

【0168】また、配信先のユーザが通常ライセンスを要求したか、プレビューライセンスを要求したかによって、発行するポイントを変更したり、自分自身がプレビューライセンスを要求した後、通常ライセンスを要求することによって、自分自身が配信元ユーザとなる場合をポイント発行から除くことなども可能となる。

【0169】それに加えて、トレーシング情報解析部45は、図17を用いて説明したトレーシング情報テーブル、および図19を用いて説明したライセンス発行テーブルを基に、ユーザの嗜好、コンテンツの配信能力、あ

10

20

30

40

50

るいは、プレビューの方法が的確であるか否かなどを、詳細に解析することが可能となる。

【0170】例えば、プレビューライセンスの要求数に対して、通常ライセンスの要求数が少ないようなコンテンツは、ユーザにとって、魅力がないコンテンツであるか、あるいは、プレビューの方法が良くない（例えば、再生箇所が的確でない、デグレードが強くて、コンテンツのよさが伝わり難いなど）という可能性がある。

【0171】それに対して、通常ライセンスの配信元ユーザIDが自分自身のユーザIDである場合、そのユーザは、プレビューライセンス要求後、通常ライセンスを要求している。そのような場合は、プレビューの方法は、的確であると考えられる。更に、通常ライセンスの配信元ユーザIDが自分自身のユーザIDではない場合、そのユーザは、プレビューライセンスを要求せずに、通常ライセンスを要求しているので、対応するコンテンツは、ユーザにとって、非常に魅力的なタイトル、あるいはアーティストであり、プレビューなしでも購入を希望するものであると考えられる。

【0172】また、配信元ユーザIDがコンテンツサーバ4となっているコンテンツに対するライセンス要求を多く送信するユーザは、コンテンツサーバ4が公開しているウェブサイトなどをこまめにチェックし、コンテンツを多くダウンロードするユーザであるといえる。

【0173】更に、通常ライセンス要求に対して、その配信元ユーザIDと配信先ユーザIDが繰り返して同一のユーザIDである場合、そのコンテンツは、同一のユーザによって、1ライセンスの規定数以上繰り返し再生されているということであるから、コンテンツの満足度が非常に高いといえる。

【0174】また、あるコンテンツを、多くの他のユーザに配信するユーザは、対応するコンテンツを気に入ったので、友人等に広く勧めていると考えられるので、コンテンツの配信状況から、ユーザの嗜好を推測することも可能となる。

【0175】更に、トレーシング情報テーブルにおいて、配信元ユーザとして多く登録されているユーザは、コンテンツの配信に積極的であるといえるが、例えば、あるコンテンツの通常ライセンスを要求していないユーザのユーザIDが、同一のコンテンツの他のユーザからのライセンス取得要求情報に多く添付されている、すなわち、トレーシング情報テーブルにおいて、配信元ユーザとして多く登録されているような場合、対応するユーザは、プレビューした結果、自分自身はあまり気に入らない場合であっても、そのコンテンツを気に入りそうなユーザに数多く配信している、すなわち、コンテンツを非常に積極的に広めようとしていることが分かる。

【0176】また、トレーシング情報テーブルにおいて、通常ライセンスに対する配信元ユーザとして多く登録されているユーザ、あるいは、通常ライセンスに対し

て配信元ユーザIDと配信先ユーザIDが同一である場合、そのコンテンツのプレビューライセンス要求時の配信元ユーザとして多く登録されているユーザは、他のユーザに対して的確にコンテンツを配信し、コンテンツの売上、すなわち通常ライセンスの要求数の向上に貢献していることが分かる。

【0177】トレーシング情報解析部45は、上述した内容以外にも、トレーシング情報テーブル、およびライセンス発行テーブルに登録されたデータを基に、更に様々な情報を解析することができる。

【0178】以上説明したように、ユーザからライセンス要求が行われる毎に、ライセンスサーバ3に、トレーシング情報の基となるユーザ情報が送信されるので、コンテンツ配信サービス事業者は、ポイントの発行など、ピアツーピアでコンテンツを他のユーザに配信したユーザに対するサービスを速やかに提供することが可能となる。これにより、コンテンツの配信を更に行おうとするユーザの意欲が高まるので、コンテンツの流通を促進することが可能となる。

【0179】ここで、ユーザのパーソナルコンピュータ1において、ライセンス取得要求情報に、コンテンツに添付されていたユーザ情報を含ませる処理、および、受信したライセンスに添付されていた自分自身のユーザ情報を、コンテンツに添付されていたユーザ情報に上書きする処理は、要求するライセンスが、プレビューライセンスであっても、通常ライセンスであっても同様の処理である。すなわち、2種類のライセンスがあるにもかかわらず、パーソナルコンピュータ1の処理は、非常に簡単であるといえる。

【0180】そして、ライセンスサーバ3において、ユーザIDが添付されたのは、プレビューライセンス取得要求情報であるか、通常ライセンス取得要求情報であるかのライセンスステータスが登録され、コンテンツIDとともに、添付されたユーザ情報に含まれるコンテンツの配信元のユーザID、および、ライセンス取得要求情報の送信元のユーザID、すなわち、コンテンツの配信先のユーザIDが、トレーシング情報テーブルに登録される。そして、ライセンス発行時に、ライセンス発行テーブルに、ライセンス取得要求情報の送信元のユーザID、コンテンツID、およびライセンスステータスが登録されるようになされている。

【0181】そして、ライセンス発行サーバ3を管理する、例えば、コンテンツ配信サービス事業者は、トレーシング情報テーブルおよびライセンス発行テーブルに登録されている情報から、コンテンツの流通経路、コンテンツの満足度、プレビューの効果、ユーザの嗜好、あるいはユーザ個々のコンテンツ配信能力などについて、非常に詳細な情報を得ることができるので、これらの情報を活用して、コンテンツの販売を促進し、顧客満足度を向上することができる。

【0182】換言すれば、ユーザのパーソナルコンピュータ1において、ライセンス取得要求情報をライセンスサーバ3に送信する時に、ライセンスとは異なる経路で入手されるコンテンツデータに添付されているユーザ情報を送信し、かつ、コンテンツデータに添付されていたユーザIDを、受信したライセンスに添付されていた自分自身のユーザIDで上書きするという非常に簡単な処理が実行されることによって、ライセンスサーバ3を管理するコンテンツ配信サービス事業者は、コンテンツの流通経路、コンテンツの満足度、プレビューの効果、ユーザの嗜好、あるいはユーザ個々のコンテンツ配信能力などについて、非常に詳細な情報を得ることができる。

【0183】また、本発明によると、通常ライセンスが要求されたときのみならず、プレビューライセンスが要求されたときにも、コンテンツの配信元ユーザのユーザIDが登録されるので、コンテンツが購入されない（通常ライセンスが要求されない）場合においても、コンテンツのトレーシングが可能である。

【0184】以上説明した処理によれば、ユーザが利用しているパーソナルコンピュータ1において、ライセンス取得要求情報がライセンスサーバ3に送信され、ライセンスを受信した場合に、対応するコンテンツに添付されているフィールドに記載されているユーザ情報を、ライセンスに含まれているユーザ情報で上書きするものとして説明しているが、例えば、ライセンスサーバ3が、ライセンスにユーザ情報を添付せず、それぞれのパーソナルコンピュータ1において、自分自身のユーザIDをライセンスサーバ3の公開鍵で暗号化してユーザ情報を作成し、コンテンツに添付されているフィールドに上書きするようにしても良い。

【0185】その場合ライセンスサーバ3の制御部41は、ライセンスステータス、ライセンスキーおよび制限情報から構成されるライセンスを、上述したように、ユーザの公開鍵で暗号化し、自分自身の署名用の秘密鍵で署名して、パーソナルコンピュータ1に送信する。

【0186】パーソナルコンピュータ1の制御部61は、自分自身のユーザIDを、メモリ63に保存しているライセンスサーバ3の公開鍵で暗号化したものを少なくとも含むユーザ情報を生成する。そして、ライセンス取得要求情報を送信したとき、もしくは、ライセンスを受信したとき、暗号化されたユーザ情報を、対応するコンテンツに添付されているフィールドに上書きする。そして、他のユーザが保有するパーソナルコンピュータに、ユーザ情報が添付されているコンテンツデータをピアツーピアで配信する。

【0187】そして、このコンテンツデータを受信したパーソナルコンピュータ1がライセンスサーバ3に送信するライセンス取得要求情報には、ライセンスサーバ3の公開鍵で暗号化されたユーザ情報が添付されているので、ライセンスサーバ3の制御部41は、暗号化および

復号処理部44を制御して、添付されているユーザ情報をライセンスサーバ3の秘密鍵を用いて復号し、トレーシング情報を得ることができる。

【0188】なお、ここでは、ユーザのパーソナルコンピュータ1とライセンスサーバ3とが授受するデータの暗号化および復号に用いる公開鍵と秘密鍵のペアと、電子署名に用いる公開鍵と秘密鍵のペアとを、それぞれ別のものとして説明したが、データの暗号化および復号用と、電子署名用の鍵のペアは、同一のものを利用するようにしても良い。

【0189】なお、ここでは、ユーザがダウンロードしたコンテンツを記録し、ライセンスキーを用いて復号して再生するためにパーソナルコンピュータ1を用いるものとして説明しているが、例えば、携帯型電話機、PDA (Personal Digital Assistant) などの各種情報処理端末や、CD (Compact Disk)、DVD (Digital Versatile Disk)、もしくはMD (Mini-Disk) (商標) などのストレージデバイス、あるいは、内部に備えたハードディスクなどの記録媒体に記録されているコンテンツデータを再生することが可能な記録再生装置などにおいても、本発明は適応することが可能である。

【0190】上述した一連の処理は、ソフトウェアにより実行することもできる。そのソフトウェアは、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、記録媒体からインストールされる。

【0191】この記録媒体は、図3に示すように、コンピュータとは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク31 (フレキシブルディスクを含む)、光ディスク32 (CD-ROM (Compact Disk-Read Only Memory)、DVD (Digital Versatile Disk) を含む)、光磁気ディスク33 (MD (Mini-Disk) (商標) を含む)、もしくは半導体メモリ34などよりなるパッケージメディアなどにより構成される。

【0192】また、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【0193】なお、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【0194】

【発明の効果】本発明の第1の情報処理装置および情報処理方法、並びにプログラムによれば、コンテンツを取得し、コンテンツに添付されている第1の情報、コンテンツを特定するための第2の情報、および自分自身を特

定することができる第3の情報を含む第4の情報を生成し、生成された第4の情報を送信し、コンテンツを再生するために必要な第5の情報を受信し、第5の情報に添付されている第6の情報を抽出し、抽出された第6の情報を、コンテンツに添付されている第1の情報に代わって、コンテンツに添付するようにしたので、コンテンツを再生するためのいわゆるライセンスの供給を受けるとともに、コンテンツの流通に関する情報をトレーシングするための情報をライセンスの供給者に送信することができる。

【0195】本発明の第2の情報処理装置および情報処理方法、並びにプログラムによれば、コンテンツを取得し、コンテンツに添付されている第1の情報、コンテンツを特定するための第2の情報、および自分自身を特定することができる第3の情報を含む第4の情報を生成し、生成された第4の情報を送信し、コンテンツを再生するために必要な第5の情報を受信し、自分自身を特定することができる第6の情報を、第4の情報の送信先の公開鍵で暗号化し、暗号化された第6の情報を、コンテンツに添付されている第1の情報に代わって、コンテンツに添付するようにしたので、コンテンツを再生するためのいわゆるライセンスの供給を受けるとともに、コンテンツの流通に関する情報をトレーシングするための情報をライセンスの供給者に送信することができる。

【0196】本発明の第3の情報処理装置および情報処理方法、並びにプログラムによれば、コンテンツを再生させるために用いられる、コンテンツに固有の第1の情報を記録し、コンテンツを保有する他の情報処理装置から、コンテンツに添付されている第2の情報、コンテンツを特定するための第3の情報、および、他の情報処理装置を特定するための第4の情報を含む第5の情報を受信し、記録されている第1の情報のうち、第3の情報によって特定されるコンテンツに対応する第1の情報を抽出し、他の情報処理装置を特定する情報を少なくとも含む第6の情報を生成し、生成された第6の情報、抽出された第1の情報を少なくとも含む第7の情報を生成し、生成された第7の情報を、第4の情報により特定される他の情報処理装置へ送信するようにしたので、ユーザにコンテンツを再生するための、いわゆるライセンスを供給するコンテンツ配信サービス事業者は、コンテンツの流通経路、コンテンツの満足度、プレビューの効果、ユーザの嗜好、あるいはユーザ個々のコンテンツ配信能力などについて分析するためのトレーシング情報を得ることが可能となる。

【0197】本発明の情報処理システムによれば、第1の情報処理装置が、コンテンツを取得し、コンテンツに添付されている第1の情報、コンテンツを特定するための第2の情報、および自分自身を特定することができる第3の情報を含む第4の情報を生成し、生成された第4の情報を第2の情報処理装置へ送信し、第2の情報処理

装置から送信されたコンテンツを再生するために必要な第5の情報を受信し、第5の情報に添付されている第6の情報を抽出し、抽出された第6の情報を、コンテンツに添付されている第1の情報に代わって、コンテンツに添付するようにし、第2の情報処理装置が、コンテンツを再生させるために用いられる、コンテンツに固有の第7の情報を記録し、第1の情報処理装置から、第1の情報、第2の情報、および、第3の情報を含む第4の情報を受信し、記録されている第7の情報のうち、第2の情報によって特定されるコンテンツに対応する第7の情報を抽出し、第1の情報処理装置を特定する情報を少なくとも含む第6の情報を生成し、生成された第6の情報、および抽出された第7の情報を少なくとも含む第5の情報を生成し、生成された第5の情報を第3の情報により特定される第1の情報処理装置へ送信するようにしたので、ユーザは、コンテンツを再生するためのいわゆるライセンスの供給を受けるとともに、コンテンツの流通に関する情報をトレーシングするための情報をライセンスの供給者に送信することができ、ライセンスを供給するコンテンツ配信サービス事業者は、コンテンツの流通経路、コンテンツの満足度、プレビューの効果、ユーザの嗜好、あるいはユーザ個々のコンテンツ配信能力などについて分析するためのトレーシング情報を得ることが可能となる。

【図面の簡単な説明】

【図1】本発明を適応したコンテンツ配信サービスを提供するために利用されるネットワーク構成図である。

【図2】コンテンツデータベースに登録されているコンテンツ管理テーブルについて説明するための図である。

【図3】パーソナルコンピュータの構成について説明するためのブロック図である。

【図4】ライセンスサーバの機能を説明するための機能ブロック図である。

【図5】ユーザ登録処理について説明するためのフローチャートである。

【図6】ユーザ登録管理テーブルについて説明するための図である。

【図7】登録ユーザが保有するパーソナルコンピュータの機能について説明するための機能ブロック図である。

【図8】パーソナルコンピュータの処理について説明するためのフローチャートである。

【図9】パーソナルコンピュータの処理について説明するためのフローチャートである。

【図10】ライセンスおよびコンテンツ、署名および暗号、並びにユーザ情報の流れについて説明するための図である。

【図11】コンテンツ管理テーブルについて説明するための図である。

【図12】ライセンスおよびコンテンツ、署名および暗号、並びにユーザ情報の流れについて説明するための図

10

20

30

40

50

である。

【図13】ライセンスおよびコンテンツ、署名および暗号、並びにユーザ情報の流れについて説明するための図である。

【図14】ライセンスおよびコンテンツ、署名および暗号、並びにユーザ情報の流れについて説明するための図である。

【図15】ライセンスサーバの処理について説明するためのフローチャートである。

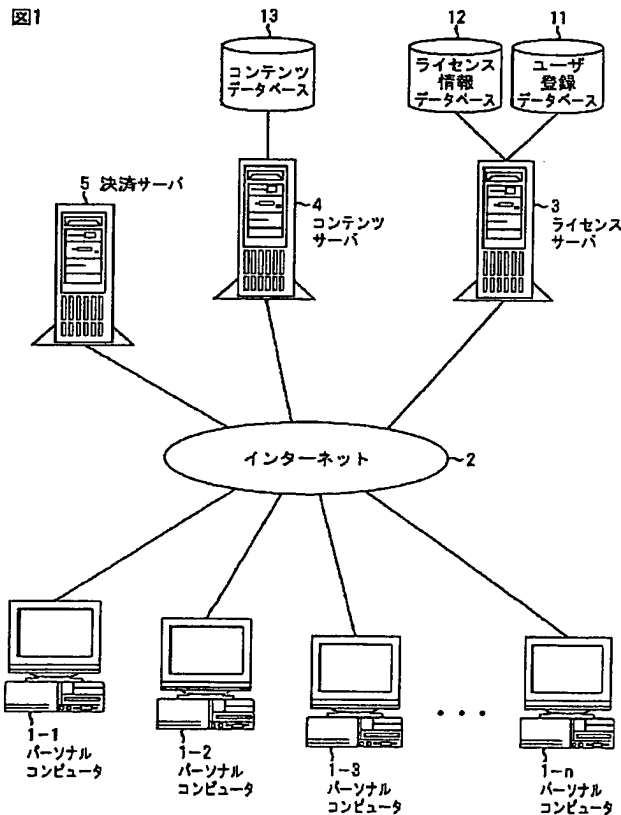
【図16】ライセンスサーバの処理について説明するためのフローチャートである。

【図17】トレーシング情報テーブルについて説明するための図である。

【図18】ライセンステーブルについて説明するための図である。

【図19】ライセンス発行テーブルについて説明するた

【図1】



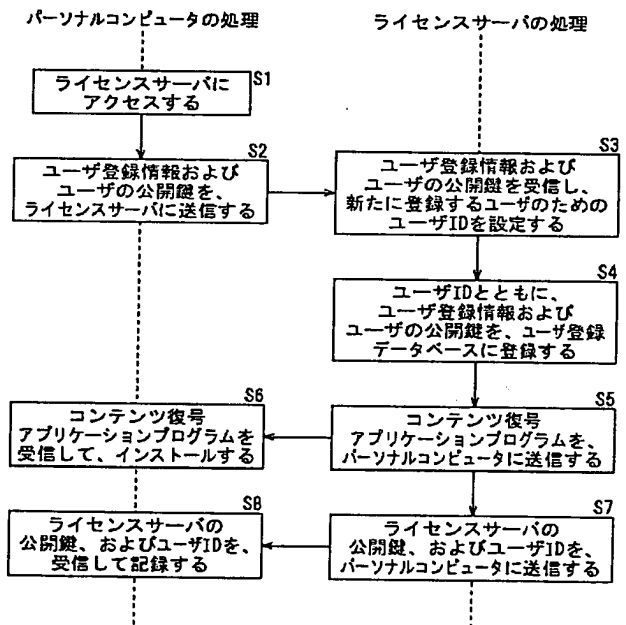
めの図である。

【符号の説明】

- 1 パーソナルコンピュータ, 2 インターネット, 3 ライセンスサーバ, 4 コンテンツサーバ, 5 決済サーバ, 11 ユーザ登録データベース, 12 ライセンス情報データベース, 13 コンテンツデータベース, 21 CPU, 24 入力部, 27 出力部, 26 RAM, 30 ネットワークインターフェース, 41 制御部, 42 入出力インターフェース, 43 メモリ, 44 暗号化および復号処理部, 45 トレーシングデータ解析部, 51 秘密鍵記録部, 61 制御部, 62 入出力インターフェース, 63 メモリ, 64 暗号化および復号処理部, 65 再生処理部, 71 秘密鍵記録部, 72 表示部, 73 スピーカ

【図5】

図5



【図2】

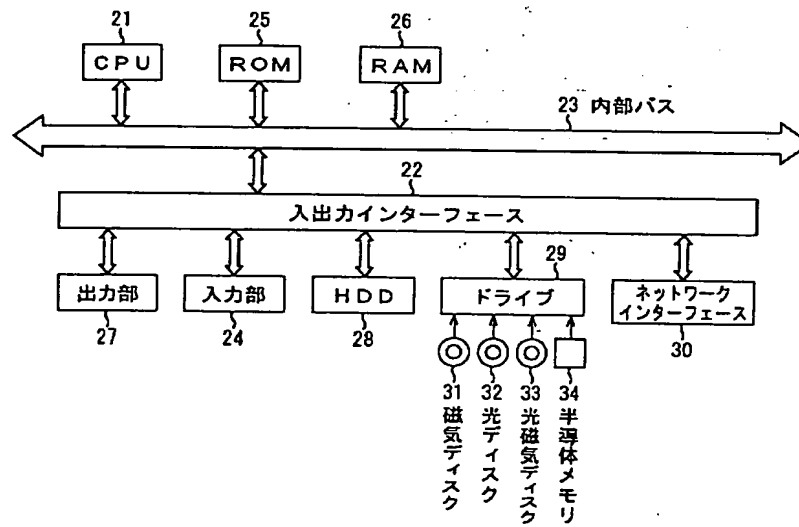
図2

コンテンツID	アドレス情報	ライセンスID	
		通常	プレビュー
000001	×××××	△△△△	〇〇〇〇
000002	×××××	△△△△	〇〇〇〇
000003	×××××	△△△△	〇〇〇〇
000004	×××××	△△△△	〇〇〇〇
000005	×××××	△△△△	〇〇〇〇
000006	×××××	△△△△	〇〇〇〇
000007	×××××	△△△△	〇〇〇〇
000008	×××××	△△△△	〇〇〇〇
⋮	⋮	⋮	⋮

コンテンツ管理テーブル

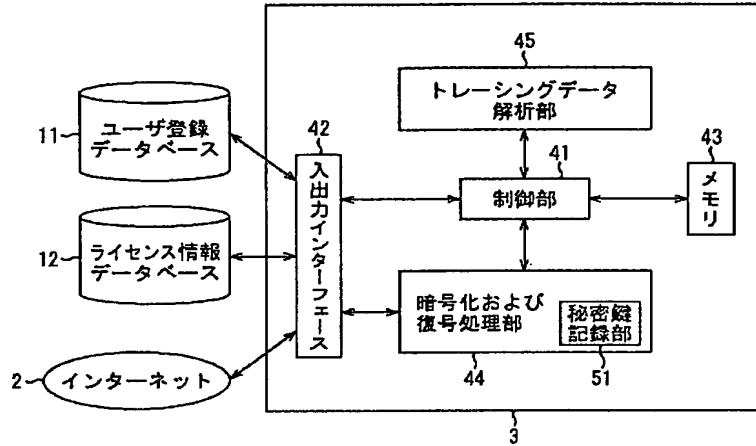
【図3】

図3



パーソナルコンピュータ 1

【図4】



【図6】

ユーザID	ユーザ公開鍵	アドレス	ユーザ情報
a0298374	〇〇〇〇	××@△△△
a0382539	〇〇〇〇	××@△△△
c7984365	〇〇〇〇	××@△△△
b4398878	〇〇〇〇	××@△△△
a1247001	〇〇〇〇	××@△△△
c8956948	〇〇〇〇	××@△△△
b8758077	〇〇〇〇	××@△△△
⋮	⋮	⋮	⋮

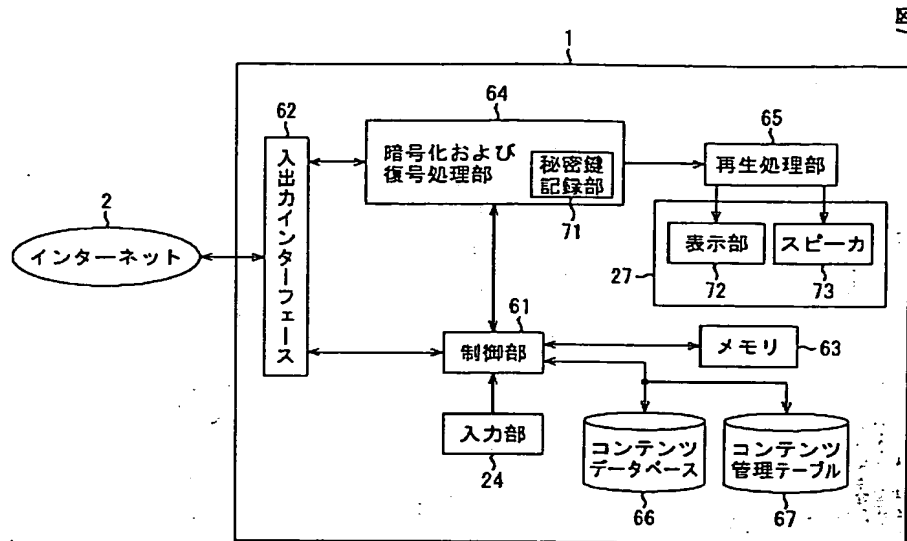
ユーザ登録管理テーブル

【図11】

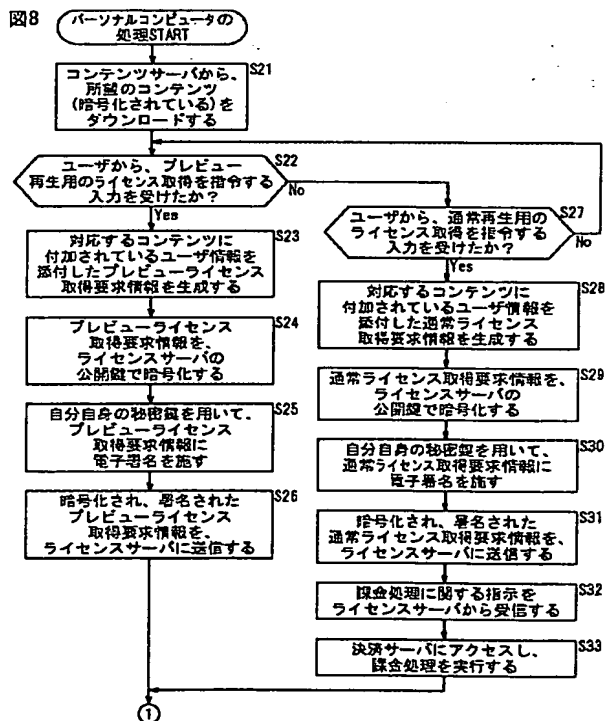
コンテンツID	アドレス情報	ライセンスID	
		通常	プレビュー
000352	×××××	△△△△	〇〇〇〇
001473	×××××		
000098	×××××		〇〇〇〇
000666	×××××		〇〇〇〇
000005	×××××	△△△△	
000543	×××××	△△△△	〇〇〇〇
⋮	⋮	⋮	⋮

コンテンツ管理テーブル

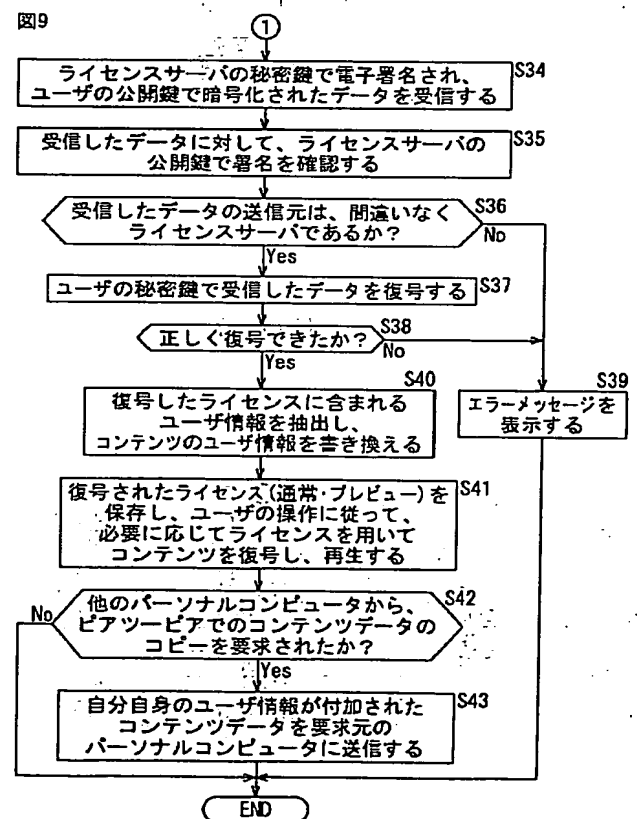
【図7】



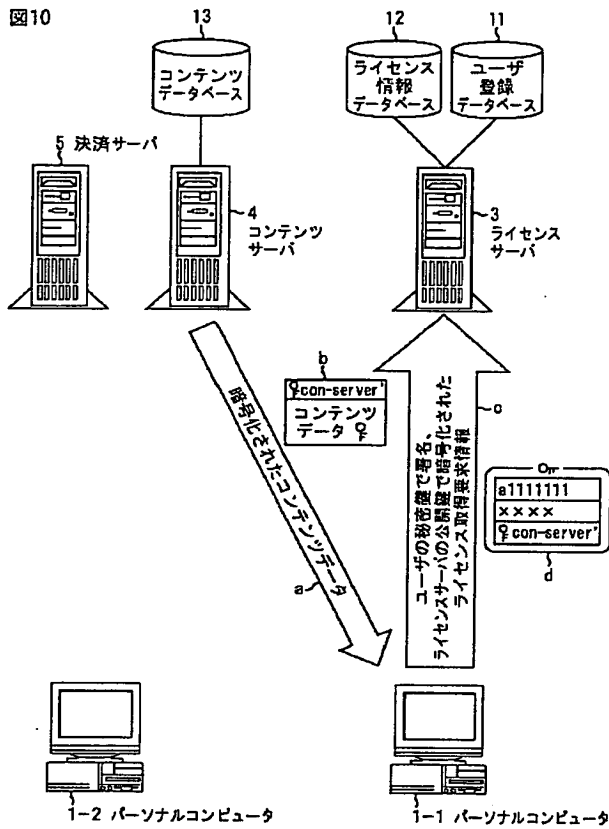
【図8】



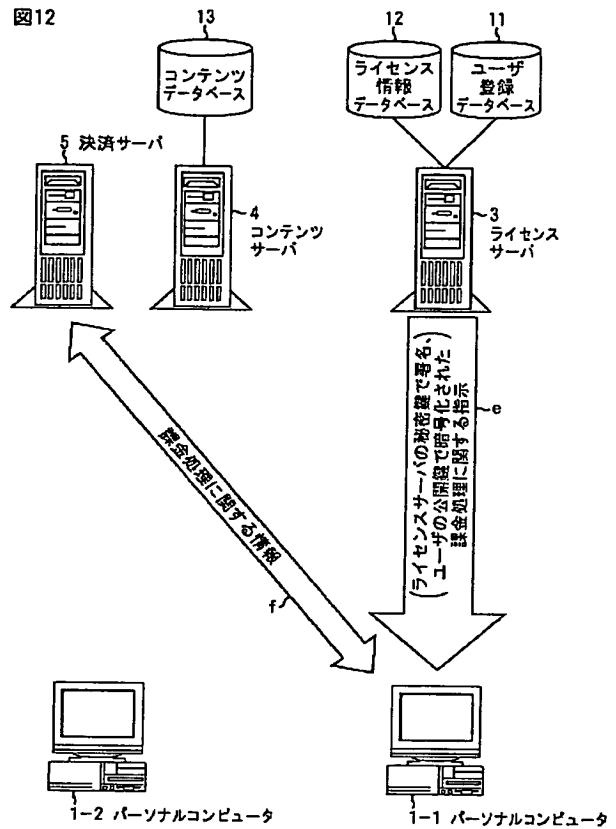
【図9】



【図 10】



【図 12】



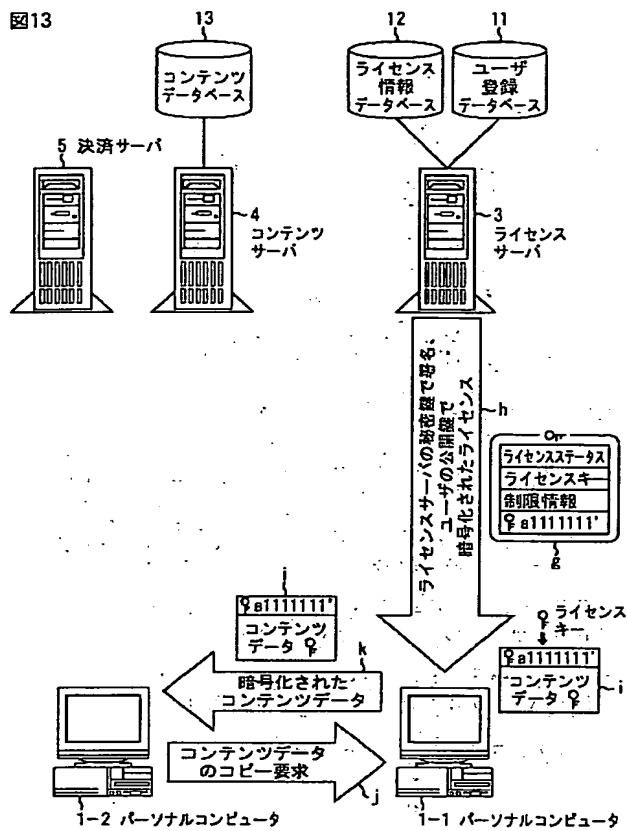
【図 17】

図 17

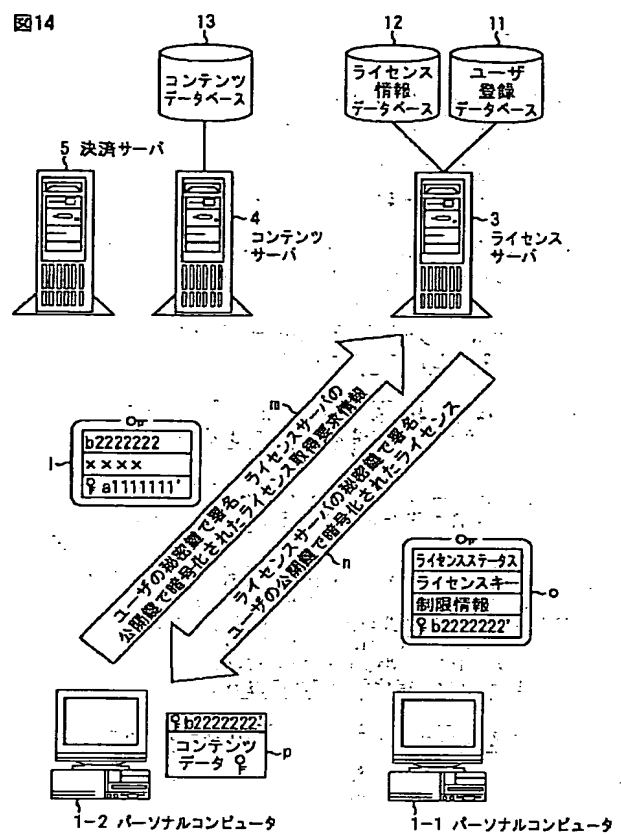
コンテンツID	ライセンスステータス	配信元ユーザID	配信先ユーザID
000005	プレビュー	con-server	a1247001
000543	プレビュー	con-server	b4398878
000098	プレビュー	a1247001	c7984365
000666	通常	c8956948	b4398878
000005	プレビュー	a1247001	a1247001
000543	通常	con-server	c8956948
000666	通常	b8758077	a0298374
000352	プレビュー	a1247001	c7984365
001473	通常	a1247001	c7984365
⋮	⋮	⋮	⋮

トレーシング情報テーブル

【圖 1 3】



【圖 14】



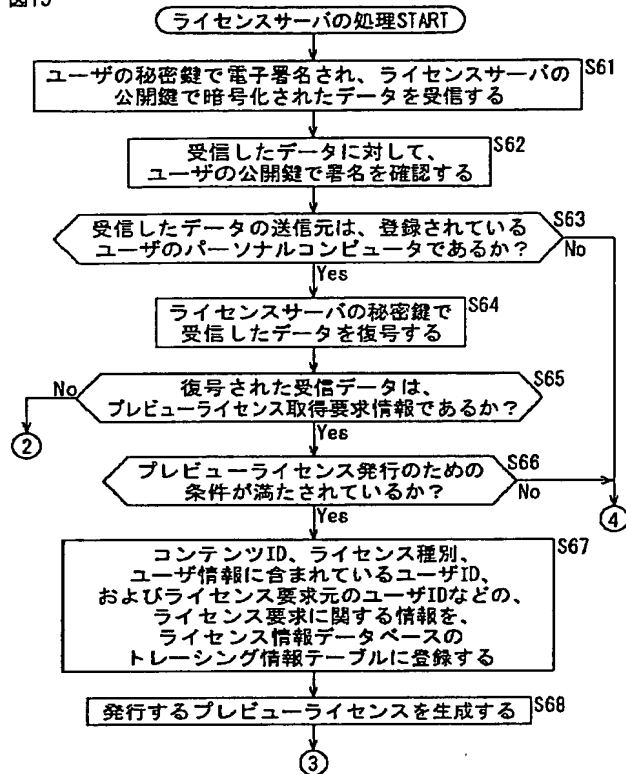
【圖 18】

コンテンツID	ライセンスID	
	通常	プレビュー
000001	△△△△	○○○○
000002	△△△△	○○○○
000003	△△△△	○○○○
000004	△△△△	○○○○
000005	△△△△	○○○○
000006	△△△△	○○○○
000007	△△△△	○○○○
000008	△△△△	○○○○
⋮	⋮	⋮

ライセンステーブル

【図15】

図15



【図19】

ユーザID	コンテンツID	ライセンスステータス
c0037472	000098	通常
a0382539	000666	通常
c7984365	000005	プレビュー
b0117837	000543	通常
a1247001	000666	プレビュー
c8956948	000670	プレビュー
b0003422	000666	プレビュー
a0111192	000005	通常
:	:	:
:	:	:

ライセンス発行テーブル

【図16】

図16

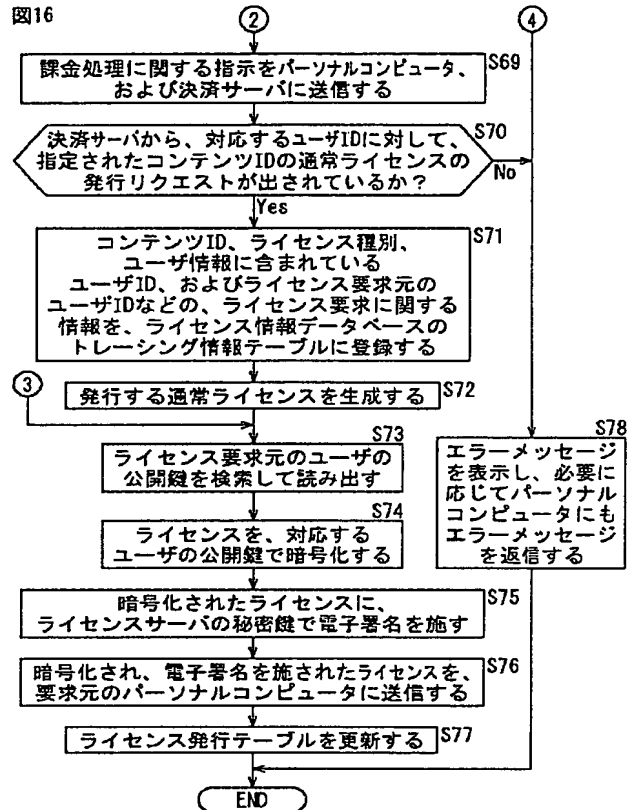


図19

フロントページの続き

(51) Int. Cl.⁷

識別記号

F I

テマコード (参考)

H 0 4 L 9/32

H 0 4 N 7/173

6 4 0 A

H 0 4 N 7/167

H 0 4 L 9/00

6 7 5 B

(29)

特開 2 0 0 3 - 1 8 7 1 0 1

7/173

6 4 0

H 0 4 N 7/167

Z

THIS PAGE BLANK (USPTO)